Monash University

Permutation Polynomials of Finite Fields

Honours Project

Author:
Christopher J. Shallue

Supervisor:
A/Prof. Ian M. Wanless

May 2012

Abstract

Let $\mathbb{F}_q$ be the finite field of q elements. Then a *permutation polynomial* (**PP**) of $\mathbb{F}_q$ is a polynomial $f \in \mathbb{F}_q[x]$ such that the associated function $c \mapsto f(c)$ is a permutation of the elements of $\mathbb{F}_q$. In 1897 Dickson gave what he claimed to be a complete list of **PP**s of degree at most 6, however there have been suggestions recently that this classification might be incomplete. Unfortunately, Dickson's claim of a full characterisation is not easily verified because his published proof is difficult to follow. This is mainly due to antiquated terminology. In this project we present a full reconstruction of the classification of degree 6 **PP**s, which combined with a recent paper by Li *et al.* finally puts to rest the characterisation problem of **PP**s of degree up to 6.

In addition, we give a survey of the major results on **PP**s since Dickson's 1897 paper. Particular emphasis is placed on the proof of the so-called *Carlitz Conjecture*, which states that if q is odd and 'large' and n is even then there are no **PP**s of degree n. This important result was resolved in the affirmative by research spanning three decades. A generalisation of Carlitz's conjecture due to Mullen proposes that if q is odd and 'large' and n is even then no polynomial of degree n is 'close' to being a **PP**. This has remained an unresolved problem in published literature. We provide a counterexample to Mullen's conjecture, and also point out how recent results imply a more general version of this statement (provided one increases what is meant by q being 'large').

Contents

Chapter 1

Permutation Polynomials of Finite Fields

This chapter is devoted to a preliminary exploration of permutation polynomials and a survey of fundamental results. Most of the ideas, results and proofs presented are based on published works of more than century's worth of academic interest in this area. In particular, the reader may find many of the theorems and proofs from this chapter in the excellent treatise on finite fields by Lidl and Neiderreiter [15, Ch. 7]. Some of the omitted proofs can also be found there. We would like to thank A. B. Evans for providing us with a preprint of his book [7], from which we have used the formula (1.2) and the proof of Theorem 1.20. Other published works have been referenced where necessary.

1.1 Functions as Polynomials

Let $q = p^r$, where p is a prime and $r \geqslant 1$ is an integer. In this project we are interested in functions from the finite field $\mathbb{F}_q$ into itself, namely functions of the form

$$\Phi : \mathbb{F}_q \longrightarrow \mathbb{F}_q.$$

To study such functions it is enough to study polynomials of degree at most $q-1$, as the next lemma shows. This result was proved by Leonard Eugene Dickson in 1897 [6]; for q prime it was already noted by Hermite [11].

Lemma 1.1. *For any function $\Phi : \mathbb{F}_q \to \mathbb{F}_q$ there exists a unique polynomial $f \in \mathbb{F}_q[x]$ of degree at most $q-1$ such that the associated polynomial function $f : c \mapsto f(c)$ satisfies $\Phi(c) = f(c)$ for all $c \in \mathbb{F}_q$.*

Proof. The following formula (*Carlitz Interpolation Formula*) gives a suitable polynomial:

$$f(x) = \sum_{c \in \mathbb{F}_q} \Phi(c) \left(1 - (x - c)^{q-1}\right). \tag{1.1}$$

To show uniqueness, suppose that $f, g \in \mathbb{F}_q[x]$ are polynomials of degree $\leqslant q - 1$ satisfying $f(c) = g(c)$ for all $c \in \mathbb{F}_q$. If $f \neq g$ then it follows that their difference $f - g$ is a nonzero polynomial that vanishes at all q elements of $\mathbb{F}_q$. But $\deg(f - g) \leqslant q - 1$, so $f - g$ can have at most $q - 1$ roots in $\mathbb{F}_q$, a contradiction. □

Note that this lemma establishes a one-to-one correspondence between functions $\Phi : \mathbb{F}_q \to \mathbb{F}_q$ and polynomials $f \in \mathbb{F}_q[x]$ of degree $\leqslant q - 1$; for there are q^q possible functions each represented uniquely by one of q^q polynomials.

Suppose that $g \in \mathbb{F}_q[x]$ is a polynomial with degree exceeding $q - 1$. Using (1.1) we can find the unique polynomial f of degree $\leqslant q - 1$ that induces the same function on the underlying field. The following lemma shows we can also find f by reduction modulo $x^q - x$.

Lemma 1.2. *For any $f, g \in \mathbb{F}_q[x]$ we have $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if $f(x) \equiv g(x)$ mod $(x^q - x)$.*

Proof. By the division algorithm we can write

$$f(x) - g(x) = h(x)(x^q - x) + r(x), \text{ where } \deg(r) < q.$$

Then $f(c) - g(c) = r(c)$ for all $c \in \mathbb{F}_q$, so $f(c) = g(c)$ for all $c \in \mathbb{F}_q$ if and only if r vanishes at every element of $\mathbb{F}_q$. Since $\deg(r) < q$ this is equivalent to $r(x) = 0$. □

1.2 Permutation Polynomials

More specifically, the objects of interest in this project are functions $f : \mathbb{F}_q \to \mathbb{F}_q$ that permute the elements of $\mathbb{F}_q$. That is, we are interested in bijections of $\mathbb{F}_q$. By Lemma 1.1 we may assume that such a function is a polynomial of degree at most $q - 1$.

Definition 1.1. A polynomial $f \in \mathbb{F}_q[x]$ is called a **Permutation Polynomial** (**PP**) of $\mathbb{F}_q$ if the associated polynomial function $f : c \to f(c)$ is a permutation of $\mathbb{F}_q$.

By the finiteness of $\mathbb{F}_q$ we can express this definition in several equivalent ways.

Lemma 1.3. *The polynomial $f \in \mathbb{F}_q[x]$ is a permutation polynomial of $\mathbb{F}_q$ if and only if one of the following conditions holds:*

(1) the function $f : c \mapsto f(c)$ is one-to-one;

(2) the function $f : c \mapsto f(c)$ is onto;

(3) $f(x) = a$ has a solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$;

(4) $f(x) = a$ has a unique solution in $\mathbb{F}_q$ for each $a \in \mathbb{F}_q$.

Example 1.1. Consider the polynomial

$$\begin{aligned} f(x) &= 3x^9 + 7x^8 + 4x^7 + 9x^6 + 8x^5 + 6x^4 + 2x^3 + 5x^2 + x + 1 \\ &= 3(x+9)(x^4 + 5x + 8)(x^4 + 8x^3 + 10x^2 + 7x + 8) \in \mathbb{F}_{11}[x]. \end{aligned}$$

By computing its values on the set $\{0, 1, ..., 10\} = \mathbb{F}_{11}$ we have

x	0	1	2	3	4	5	6	7	8	9	10
$f(x)$	1	2	0	3	4	5	6	7	8	9	10

Since $f(x)$ is a bijection it is a permutation polynomial of $\mathbb{F}_{11}$, and we observe that it represents the 3-cycle $(0, 1, 2)$. □

Example 1.2. Consider the polynomial

$$g(x) = x^3 + 1 \in \mathbb{F}_{11}[x].$$

As in the previous example we check whether g is a **PP** of $\mathbb{F}_{11}$ by computing its values on $\mathbb{F}_{11}$. We get

x	0	1	2	3	4	5	6	7	8	9	10
$g(x)$	1	2	9	6	10	5	8	3	7	4	0

We see that g is a **PP** of $\mathbb{F}_{11}$ with cycle structure $(0, 1, 2, 9, 4, 10)(3, 6, 8, 7)$. □

Example 1.3. Finally, consider the polynomial

$$h(x) = x^2 + 3x + 5 \in \mathbb{F}_{11}[x],$$

which takes the values

x	0	1	2	3	4	5	6	7	8	9	10
$h(x)$	5	9	4	1	0	1	4	9	5	3	3

We see that $h(x)$ is *not* a **PP** of $\mathbb{F}_{11}$. This is also clear if we write h in the form

$$h(x) = (x + 7)^2,$$

and observe that since x^2 is not an onto function neither is any function composed with x^2. □

Remark 1.1. Examples 1.1 and 1.2 demonstrate a noteworthy fact on the relationship between permutations and their associated polynomials: simplicity of cycle structure does not imply simplicity as a polynomial, and vice versa. In fact, let $a, b \in \mathbb{F}_q$ and consider the transposition (a, b); the permutation with simplest non-trivial cycle structure. By (1.1) we determine that the **PP** representing (a, b) is given by

$$f(x) = x + (b-a)(1-(x-a)^{q-1}) + (a-b)(1-(x-b)^{q-1}). \tag{1.2}$$

Clearly, this is a more complex structure than its cycle form.

In fact, it is true in general that permutations with simple cycle structure tend to have complex polynomial structure. The interested reader may refer to [33], which shows that most permutations that move very few elements have maximum possible degree. For example, all transpositions and almost all 3-cycles have maximal degree.

1.3 Criteria for Permutation Polynomials

Given a polynomial $f \in \mathbb{F}_q[x]$ it is natural to ask: is $f(x)$ a **PP** of $\mathbb{F}_q$? For an arbitrary polynomial f this is a difficult question to answer. A straightforward approach (as in Examples 1.1 - 1.3) is to evaluate $f(c)$ for each $c \in \mathbb{F}_q$, and determine by examination whether or not f is a bijection. If q and $\deg(f)$ are small this is plausible, however in general it is computationally impractical. Although there do exist other techniques, all currently known criteria for **PP**s are complicated by way of requiring long calculations. There are no methods that allow an arbitrary polynomial to be checked by inspection, for example.

In this section we aim to give a fairly comprehensive survey of all known criteria for **PP**s. First we give considerable attention to a classical result known as Hermite's criterion. This theorem was first given by Hermite for fields of prime order [11], and was later generalised by Dickson to general finite fields [6]. We will use this theorem extensively in Chapter 3.

1.3.1 Hermite's Criterion

Permutation polynomials of $\mathbb{F}_q$ may be characterised as polynomial functions $f \in \mathbb{F}_q[x]$ satisfying the property

$$\{f(c) : c \in \mathbb{F}_q\} = \mathbb{F}_q.$$

Hence, it is useful to have a characterisation of sequences $a_0, a_1, ..., a_{q-1}$ of elements of $\mathbb{F}_q$ that satisfy $\{a_0, a_1, ..., a_{q-1}\} = \mathbb{F}_q$. Note that the set $\{f(c) : c \in \mathbb{F}_q\}$ is known as the *value set of* f, denoted V_f, and will be discussed further in Chapter 2.

For the following lemma we must first recall the formula for the sum of the first n terms of a geometric series. Let F be a field and let $a \in F$, $a \neq 1$. Then the following identity holds

$$\sum_{i=0}^{n-1} a^i = \frac{(1-a^n)}{1-a}. \tag{1.3}$$

Lemma 1.4. *The sequence* $a_0, ..., a_{q-1}$ *of elements of* $\mathbb{F}_q$ *satisfies* $\{a_0, ..., a_{q-1}\} = \mathbb{F}_q$ *if and only if*

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \textit{for } t = 0, 1, ..., q-2, \\ -1 & \textit{for } t = q-1. \end{cases}$$

Proof. For each $0 \leqslant i \leqslant q-1$ consider the polynomial

$$g_i(x) = 1 - \sum_{t=0}^{q-1} a_i^t x^{q-1-t}.$$

It is clear that $g_i(a_i) = 1$ for all $0 \leqslant i \leqslant q-1$. Note that we also have $g_i(b) = 0$ for all $b \in \mathbb{F}_q, b \neq a_i$. To show this, suppose that $b \neq 0$. Then by (1.3) we have

$$g_i(b) = 1 - \sum_{t=0}^{q-1} a_i^t b^{q-1-t} = 1 - \sum_{t=0}^{q-1} (a_i b^{-1})^t = 1 - \frac{1-(a_i b^{-1})^q}{1-(a_i b^{-1})} = 1 - 1 = 0.$$

Moreover it is clear that $g_i(0) = 0$ whenever $a_i \neq 0$. Hence the polynomial

$$g(x) = \sum_{i=0}^{q-1} g_i(x) = -\sum_{i=0}^{q-1} \left(\sum_{t=0}^{q-1} a_i^t x^{q-1-t} \right) = -\sum_{t=0}^{q-1} \left(\sum_{i=0}^{q-1} a_i^t \right) x^{q-1-t} \tag{1.4}$$

satisfies

$$g(x) = \begin{cases} 1 & \text{if } x \in \{a_0, a_1, ..., a_{q-1}\}, \\ 0 & \text{if } x \in \mathbb{F}_q \setminus \{a_0, a_1, ..., a_{q-1}\}. \end{cases}$$

So $g(x)$ maps every element of $\mathbb{F}_q$ to 1 if and only if $\{a_0, a_1, ..., a_{q-1}\} = \mathbb{F}_q$. But since $\deg(g) \leqslant q-1$ we have by Lemma 1.1 that g maps every element to 1 if and only if $g(x) = 1$, which by (1.4) is equivalent to

$$\sum_{i=0}^{q-1} a_i^t = \begin{cases} 0 & \text{for } t = 0, 1, ..., q-2, \\ -1 & \text{for } t = q-1. \end{cases}$$

□

The following criterion for permutation polynomials is known as Hermite's criterion.

Theorem 1.5. (Hermite's criterion.) *Let $q = p^r$, where p is a prime and r is a positive integer. Then a polynomial $f \in \mathbb{F}_q[x]$ is a* **PP** *of $\mathbb{F}_q$ if and only if the following two conditions hold:*

(1) the reduction of $f(x)^{q-1}$ mod $(x^q - x)$ is monic of degree $q-1$;

(2) for each integer t with $1 \leqslant t \leqslant q-2$ and $t \not\equiv 0$ mod p, the reduction of $f(x)^t$ mod $(x^q - x)$ has degree $\leqslant q-2$.

Proof. For each $1 \leqslant t \leqslant q-1$, denote the reduction of $f(x)^t$ modulo $x^q - x$ by

$$f(x)^t \bmod (x^q - x) = \sum_{i=0}^{q-1} b_i^{(t)} x^i.$$

Note that by (1.1) we have $b_{q-1}^{(t)} = -\sum_{c\in\mathbb{F}_q} f(c)^t$.

Suppose that $f(x)$ is a **PP** of $\mathbb{F}_q$. Then since $\{f(c) : c \in \mathbb{F}_q\} = \mathbb{F}_q$ we have by Lemma 1.4 that $b_{q-1}^{(t)} = 0$ for all $1 \leqslant t \leqslant q-2$ and $b_{q-1}^{(q-1)} = 1$.

Now suppose that (1) and (2) are satisfied. Then (1) implies that $-b_{q-1}^{(q-1)} = \sum_{c\in\mathbb{F}_q} f(c)^{q-1} = -1$, whilst (2) implies that $-b_{q-1}^{(t)} = \sum_{c\in\mathbb{F}_q} f(c)^t = 0$ for all $1 \leqslant t \leqslant q-2$, $t \not\equiv 0$ mod p. If $t \equiv 0$ mod p we may write $t = t'p^j$, where $1 \leqslant t' \leqslant q-2$ and $t' \not\equiv 0$ mod p. We then have

$$\sum_{c\in\mathbb{F}_q} f(c)^t = \sum_{c\in\mathbb{F}_q} f(c)^{t'p^j} = \left(\sum_{c\in\mathbb{F}_q} f(c)^{t'}\right)^{p^j} = 0.$$

So $\sum_{c\in\mathbb{F}_q} f(c)^t = 0$ for all $1 \leqslant t \leqslant q-2$ and this identity also holds trivially for $t = 0$. By Lemma 1.4, $f(x)$ is a **PP** of $\mathbb{F}_q$. □

In the previous proof it is possible to remove the condition that the reduced polynomial in (1) is monic; it is enough to say that its degree is $q-1$. Alternatively, we can replace condition (1) in Theorem 1.5 by other conditions. The following theorem is an equivalent form of Hermite's criterion, and in fact is very close to the original statement proved by Dickson in 1897.

Theorem 1.6. *Let $q = p^r$, where p is a prime and r is a positive integer. Then a polynomial $f \in \mathbb{F}_q[x]$ is a* **PP** *of $\mathbb{F}_q$ if and only if the following two conditions hold:*

(1) f has exactly one root in $\mathbb{F}_q$;

(2) for each integer t with $1 \leqslant t \leqslant q-2$ and $t \not\equiv 0$ mod p, the reduction of $f(x)^t$ mod $(x^q - x)$ has degree $\leqslant q-2$.

Proof. We wish to prove that f has exactly one root in $\mathbb{F}_q$ if and only if the reduction of $f(x)^{q-1} \bmod (x^q - x)$ is monic of degree $q-1$. As in the proof of Theorem 1.5 we write

$$f(x)^t \bmod (x^q - x) = \sum_{i=0}^{q-1} b_i^{(t)} x^i,$$

where $b_{q-1}^{(t)} = -\sum_{c\in\mathbb{F}_q} f(c)^t$. Suppose that f has exactly j roots in $\mathbb{F}_q$. Then

$$b_{q-1}^{(q-1)} = -\sum_{c\in\mathbb{F}_q} f(c)^{q-1} = -(q-j) = j,$$

and since $0 \leqslant j \leqslant q-1$ we have $b_{q-1}^{(q-1)} = 1$ if and only if $j = 1$. □

Hermite's criterion gives us some immediate and very useful corollaries. We first show that every reduced **PP** of $\mathbb{F}_q$ must have degree $\leqslant q-2$.

Corollary 1.7. *If $q > 2$ and $f(x)$ is a* **PP** *of $\mathbb{F}_q$ then the reduction of f modulo $x^q - x$ has degree at most $q-2$.*

Proof. Set $t = 1$ in Theorem 1.5. □

Corollary 1.8. *If $q \equiv 1 \bmod n$ then there is no* **PP** *of $\mathbb{F}_q$ of degree n.*

Proof. Let $f(x) \in \mathbb{F}_q[x]$, where $q = p^r = nm+1$ for some positive integer m. By Lemma 1.2 we may assume that $n \leqslant q-1$. Then $1 \leqslant m \leqslant q-1$ for all $n \geqslant 1$, and $m \not\equiv 0 \bmod p$ (otherwise $0 \equiv 1 \bmod p$). But $\deg(f(x)^m) = nm = q-1$, so by Theorem 1.5 $f(x)$ is not a **PP** of $\mathbb{F}_q$. □

1.3.2 Survey of Known Criteria

Recall that a *character* χ of a finite abelian group G is a homomorphism from G into the multiplicative group U of complex numbers of unit absolute value. The number of characters of G is equal to $|G|$. If $\mathbb{F}_q$ is a finite field then an *additive character* of $\mathbb{F}_q$ is a character of the additive group of $\mathbb{F}_q$, that is, a function $\chi : \mathbb{F}_q \to U$ such that

$$\chi(x_1 + x_2) = \chi(x_1)\chi(x_2) \text{ for all } x_1, x_2 \in \mathbb{F}_q.$$

The *trivial additive character* χ_0 of $\mathbb{F}_q$ is defined by $\chi_0(c) = 1$ for all $c \in \mathbb{F}_q$; all other additive characters are considered nontrivial.

The following characterisation of **PP**s of $\mathbb{F}_q$ is well known, see for example [15].

Theorem 1.9. *A polynomial $f \in \mathbb{F}_q[x]$ is a* **PP** *of $\mathbb{F}_q$ if and only if*

$$\sum_{c\in\mathbb{F}_q} \chi(f(c)) = 0$$

for all nontrivial additive characters χ of $\mathbb{F}_q$.

The following characterisation of **PP**s dates back to 1883 and is due to Raussnitz. The version given here is from [23], where the reader may also find its proof. The same theorem can also be found in [17, p. 133]. We have included a reference to the original paper of Raussnitz [20], however we remark that we were not able to find a copy.

Recall that the *circulant matrix* with first row $(a_0, ..., a_n)$ is defined by

$$M = \begin{pmatrix} a_0 & a_1 & \cdots & a_n \\ a_n & a_0 & \cdots & a_{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & \cdots & a_0 \end{pmatrix}.$$

Theorem 1.10. (Raussnitz). *Consider the polynomial $f(x) = \sum_{i=0}^{q-2} a_i x^i$ and let M_f be the circulant matrix with first row $(a_0, a_1, ..., a_{q-2})$. Then $f(x)$ is a* **PP** *of $\mathbb{F}_q$ if and only if the characteristic polynomial of M_f is $(x - a_0)^{q-1} - 1$.*

In [24] the author derives the following criterion equivalent to the theorem of Raussnitz. If $f(x) = \sum_{i=0}^{n} a_i x^i$ and $g(x) = \sum_{i=0}^{m} b_i x^i$, define the *Sylvester matrix* of f and g by

$$R(f,g) = \begin{pmatrix} a_n & a_{n-1} & \cdots & a_0 & & & \\ & a_n & a_{n-1} & \cdots & a_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & a_n & a_{n-1} & \cdots & a_0 \\ b_m & b_{m-1} & \cdots & b_0 & & & \\ & b_m & b_{m-1} & \cdots & b_0 & & \\ & & \ddots & \ddots & & \ddots & \\ & & & b_m & b_{m-1} & \cdots & b_0 \end{pmatrix}.$$

Theorem 1.11. *Let $f \in \mathbb{F}_q[x]$ and let*

$$g_f = \det\left(R(x^q - x, f - y)\right) - (-1)^q (y^q - y) \in \mathbb{F}_q[y].$$

Then $f(x)$ is a **PP** *of $\mathbb{F}_q$ if and only if $g_f = 0$.*

By studying elementary symmetric polynomials, Turnwald [23, Theorem 2.13] proves a theorem giving no less than nine characterisations of **PP**s. Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree n such that $1 \leqslant n < q$ and let s_k be the k^{th} elementary symmetric polynomial of the values $f(c)$, that is,

$$\prod_{c \in \mathbb{F}_q} (x - f(c)) = \sum_{k=0}^{q} (-1)^k s_k x^{q-k}. \tag{1.5}$$

Let u be the smallest positive integer k such that $s_k = 0$ and let w be the smallest positive integer k such that $p_k = \sum_{c \in \mathbb{F}_q} f(c)^k \neq 0$. Let v be the number of distinct values of f. In [23] the author studies the relationships between the values u, v, w, n and q, in particular deriving the following characterisations of the statement $v = q$ (i.e. f is a **PP**).

Theorem 1.12. *Let $f \in \mathbb{F}_q[x]$ be a polynomial of degree n with $1 \leqslant n < q$ and let u, w, v be as defined above. Then the following statements are equivalent:*

(1) $f(x)$ *is a* **PP**.

(2) $u = q - 1$.

(3) $u > q - q/n$.

(4) $u > q - v$.

(5) $v > q - (q-1)/n$.

(6) $w = q - 1$.

(7) $2q/3 - 1 < w < \infty$.

(8) $q - (q+1)/n < w < \infty$.

(9) $q - u \leqslant w < \infty$.

(10) $u > (q-1)/2$ *and* $w < \infty$.

The remarkable fact that $v > q - (q-1)/n$ implies $v = q$ is a theorem due to Wan, which we will discuss further in Chapter 2.

For completeness of this survey we give a final criterion that has been reported in the literature. According to a statement in [18, p. 251], the following theorem is taken from a preprint of Moreno *et al.*, however it does not seem that the paper in question was published. The reference of this preprint may be found in the bibliography of [18].

Theorem 1.13. *A polynomial $f \in \mathbb{F}_q[x]$ is a* **PP** *of $\mathbb{F}_q$ if and only if one of the following conditions holds:*

(1) $(f(x) - c)^{q-1} \not\equiv 1$ *mod* $(x^q - x)$ *for all* $c \in \mathbb{F}_q$.

(2) $(f(x) - f(c))^{q-1} \equiv (x - c)^{q-1}$ *mod* $(x^q - x)$ *for all* $c \in \mathbb{F}_q$.

At the conclusion of this section we remark that all the criteria listed here are computationally demanding, even for polynomials of small degrees over small fields. For this reason, some of the above criteria have been converted into probabilistic algorithms for testing for **PP**s. In particular, the reader is referred to [24] for probabilistic versions of Theorem 1.6 and Theorem 1.11. See also [25, 21].

1.4 Classes of Permutation Polynomials

We have seen that in general it is difficult to tell whether or not an arbitrary polynomial is a **PP**. However, for certain special classes of polynomials this question is easier to answer. In this section we give a survey of the major known classes.

The following are elementary classes of **PP**s.

Theorem 1.14.

(1) *Every linear polynomial over* $\mathbb{F}_q$ *is a* **PP** *of* $\mathbb{F}_q$.

(2) *The monomial* x^n *is a* **PP** *of* $\mathbb{F}_q$ *if and only if* $\gcd(n, q-1) = 1$.

Proof. (1) Trivial. (2) Since $0^n = 0$ the monomial x^n is onto if and only if the function $f : \mathbb{F}_q^\times \to \mathbb{F}_q^\times, x \mapsto x^n$ is onto. Let g be a primitive element of the cyclic group $\mathbb{F}_q^\times$. Then the image of $\mathbb{F}_q^\times$ under f is the cyclic subgroup generated by g^n, which equals $\mathbb{F}_q^\times$ if and only if g^n is a primitive element. This is equivalent to the statement $\gcd(n, q-1) = 1$. □

We now consider a class of polynomials known as q-polynomials. Let $q = p^r$ where p is a prime and r is a positive integer. Then a polynomial of the form

$$L(x) = \sum_{i=0}^{n} a_i x^{q^i} = a_0 x + a_1 x^q + \cdots + a_n x^{q^n} \in \mathbb{F}_{q^m}[x]$$

is called a ***q*-polynomial** over $\mathbb{F}_{q^m}$. Such polynomials are also known as *linearised polynomials*, whose name stems from the properties

(1) $L(\beta + \gamma) = L(\beta) + L(\gamma)$ for all $\beta, \gamma \in \mathbb{F}_{q^m}$,

(2) $L(c\beta) = cL(\beta)$ for all $c \in \mathbb{F}_q, \beta \in \mathbb{F}_{q^m}$.

We remark that properties (1) and (2) hold more generally for β, γ in an arbitrary extension field of $\mathbb{F}_{q^m}$. If $\mathbb{F}_{q^m}$ is considered as a vector space over $\mathbb{F}_q$ then these properties show that $L(x)$ is a linear operator on $\mathbb{F}_{q^m}$.

The following theorem classifies when a p-polynomial is a **PP**.

Theorem 1.15. *Let* $\mathbb{F}_q$ *be of characteristic* p. *Then the* p*-polynomial*

$$L(x) = \sum_{i=0}^{m} a_i x^{p^i} \in \mathbb{F}_q[x]$$

is a **PP** *if and only if* $L(x)$ *only has the root 0 in* $\mathbb{F}_q$.

Proof. Necessity is obvious. Suppose that $L(x)$ only has the root zero. Then by the discussion above we have $L(a) = L(b)$ if and only if $L(a - b) = 0$. But since zero is the only root of $L(x)$ we must then have $a = b$. So $L(x)$ is one-to-one, so it is a **PP** (Lemma 1.3). □

We have a second criterion that applies to a class of q-polynomials.

Theorem 1.16. *Let $\mathbb{F}_{q^m}$ be an extension of $\mathbb{F}_q$ and consider polynomials of the form*

$$L(x) = \sum_{i=0}^{m-1} a_i x^{q^i} \in \mathbb{F}_{q^m}[x].$$

Then $L(x)$ is a **PP** *of $\mathbb{F}_{q^m}$ if and only if* $\det(A) \neq 0$*, where*

$$A = \begin{pmatrix} a_0 & a_{m-1}^q & a_{m-2}^{q^2} & \cdots & a_1^{q^{m-1}} \\ a_1 & a_0^q & a_{m-1}^{q^2} & \cdots & a_2^{q^{m-1}} \\ a_2 & a_1^q & a_0^{q^2} & \cdots & a_3^{q^{m-1}} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{m-1} & a_{m-2}^q & a_{m-3}^{q^2} & \cdots & a_0^{q^{m-1}} \end{pmatrix}.$$

If each a_i is an element of $\mathbb{F}_q$ then $L(x)$ is a **PP** *of $\mathbb{F}_{q^m}$ if and only if*

$$\gcd\left(\sum_{i=0}^{m-1} a_i x^i, x^i - 1\right) = 1.$$

If $\mathbb{F}_q$ is a finite field then polynomials that are **PP**s of *all* finite extensions of $\mathbb{F}_q$ are very rare. The following theorem gives the complete classification of polynomials with this property, which is in fact a special class of p-polynomial.

Theorem 1.17. *Let $q = p^r$ where p is a prime and r is a positive integer. Then a polynomial $f \in \mathbb{F}_q[x]$ is a* **PP** *of all finite extensions of $\mathbb{F}_q$ if and only if it is of the form $f(x) = ax^{p^h} + b$, where $a \neq 0$ and h is a nonnegative integer.*

Proof. Let $\mathbb{F}_{q^m}$ be a finite extension of $\mathbb{F}_q$. If $c = a^{-1}b$ then we have

$$f(x) = ax^{p^h} + b = a(x^{p^h} + c) = a(x + c)^{p^h}.$$

Then $f(x) = h \circ g$, where $g(x) = x + c$ is a **PP** of $\mathbb{F}_{q^m}$ by Theorem 1.14 and $h(x) = ax^{p^h}$ is a **PP** of $\mathbb{F}_{q^m}$ by Theorem 1.15. Hence, $f(x)$ is a **PP** of $\mathbb{F}_{q^m}$. For necessity see [15]. □

Corollary 1.18. *If $f \in \mathbb{F}_q[x]$ is not of the form $f(x) = ax^{p^h} + b$ then there are infinitely many extension fields $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ such that f is not a permutation polynomial of $\mathbb{F}_{q^m}$.*

The next theorem gives a class of **PP**s of a very specific form.

Theorem 1.19. *Let h be a positive integer with* $\gcd(h, q-1) = 1$ *and let s be a positive divisor of $q - 1$. Let $g \in \mathbb{F}_q[x]$ be such that $g(x^s)$ has no nonzero root in $\mathbb{F}_q$. Then the polynomial*

$$f(x) = x^h (g(x^s))^{(q-1)/s}$$

is a **PP** *of $\mathbb{F}_q$.*

Proof. We use Theorem 1.6. Clearly condition (1) is satisfied. Let $1 \leqslant t \leqslant q-2$ and suppose that s does not divide t. Now, all exponents of $f(x)^t$ are of the form $ht+ms$ for some positive integer m, and since $\gcd(h,s)=1$ none of these exponents is divisible by s. Hence no exponents are divisible by $q-1$. So there are no terms of the form $x^{i(q-1)}$ in the expansion of $f(x)^t$, so the reduction of $f(x)^t$ has degree $\leqslant q-2$.

Now suppose that $t=ks$ for some positive integer k. Then we have

$$f(x)^t = x^{ht}(g(x^s))^{(q-1)k}.$$

For all $c \in \mathbb{F}_q^\times$ we have $f(c)=c^{ht}$ (because $g(c^s) \neq 0$), and for $c=0$ we have $f(0)=0=0^{ht}$. By Lemma 1.2 we have

$$f(x)^t \equiv x^{ht} \bmod (x^q-x),$$

and since $q-1$ does not divide ht the monomial x^{ht} reduces modulo x^q-x to a polynomial of degree $\leqslant q-2$. □

The following theorem completely classifies **PP**s of the form $x^{(q+1)/2}+ax$ for odd q. As is the case with many families of permutation polynomials (see Table A.1), whether or not a polynomial family parametrised by a is a **PP** often depends on the *quadratic character* of a; that is, whether or not a is a square in $\mathbb{F}_q$. The following theorem is the first place we encounter this.

We remind the reader that for all $x \in \mathbb{F}_q^\times$ we have

$$x^{(q-1)/2} = \begin{cases} 1 & \text{if } x \text{ is a square,} \\ -1 & \text{if } x \text{ is a nonsquare.} \end{cases} \tag{1.6}$$

Theorem 1.20. *If q is odd then the polynomial $x^{(q+1)/2}+ax \in \mathbb{F}_q[x]$ is a* **PP** *of $\mathbb{F}_q$ if and only if a^2-1 is a nonzero square.*

Proof. Note that $f(x)=x^{(q+1)/2}+ax=(x^{(q-1)/2}+a)x$, so we have by (1.6)

$$f(x) = \begin{cases} (a+1)x & \text{if } x \text{ is a nonzero square,} \\ (a-1)x & \text{if } x \text{ is a nonsquare,} \\ 0 & \text{if } x=0. \end{cases} \tag{1.7}$$

If $a^2-1=0$ then $a=\pm 1$, in which case $f(x)$ has repeated roots by (1.7). So we may assume that $a \notin \{1,-1\}$. Now (1.7) shows that the image of $\mathbb{F}_q$ under f is given by

$$\{(a-1)x : x \in \mathbb{F}_q^\times \text{ is a nonsquare}\} \cup \{(a+1)x : x \in \mathbb{F}_q^\times \text{ is a square}\} \cup \{0\}.$$

The first set contains precisely the squares in $\mathbb{F}_q^\times$ if $a-1$ is a square, and precisely the nonsquares in $\mathbb{F}_q^\times$ if $a-1$ is a nonsquare. Similarly, the second set contains precisely the nonsquares in $\mathbb{F}_q^\times$ if $a+1$ is a square, and precisely the squares in $\mathbb{F}_q^\times$ if $a+1$ is a nonsquare. Hence, $f(x)$ is onto $\mathbb{F}_q$ if and only if $a-1$ and $a+1$ are either both squares or both nonsquares. We can state this condition more compactly as

$$(a-1)(a+1) = a^2 - 1 \text{ is a nonzero square.}$$

□

The more general class of polynomials of the form $x^{(q+m-1)/m} + ax$, where m is a positive divisor of $q-1$, have also been classified.

Theorem 1.21. *Let $m > 1$ be a divisor of $q-1$. Then the polynomial $f(x) = x^{(q+m-1)/m} + ax \in \mathbb{F}_q[x]$ is a* **PP** *of $\mathbb{F}_q$ if and only if $(-a)^m \neq 1$ and*

$$\left(\frac{a+\xi^i}{a+\xi^j}\right)^{\frac{q-1}{m}} \neq \xi^{j-i} \text{ for all } 0 \leqslant i < j < m,$$

where ξ is a fixed primitive m^{th} root of unity in $\mathbb{F}_q$.

We now introduce a class of polynomials known as *Dickson polynomials.*

Definition 1.2. Let R be a commutative ring with identity. For $a \in R$ define the **Dickson polynomial** $g_k(x,a)$ of degree k over R by

$$g_k(x,a) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-a)^j x^{k-2j}.$$

Dickson polynomials satisfy a number of interesting properties, for example we have $g_1(x,a) = x$, $g_2(x,a) = x^2 - 2a$, and

$$g_{k+1}(x,a) = x g_k(x,a) - a g_{k-1}(x,a), \text{ for } k \geqslant 2.$$

We refer the reader to [15] for more interesting properties of $g_k(x,a)$. The following theorem characterises when Dickson polynomials are **PP**s. Remarkably, whether or not the Dickson polynomial $g_k(x,a)$ is a **PP** of $\mathbb{F}_q$ depends only on its degree (not on a).

Theorem 1.22. *Let $a \in \mathbb{F}_q^\times$. Then the Dickson polynomial $g_k(x,a)$ is a* **PP** *of $\mathbb{F}_q$ if and only if* $\gcd(k, q^2-1) = 1$.

An interesting perspective of Dickson polynomials is that they generalise the power polynomial x^k. Because $g_k(x,0) = x^k$, which by Theorem 1.14 is a **PP** of $\mathbb{F}_q$ if and only if $\gcd(k, q-1) = 1$. On the other hand, if $a \neq 0$ then the polynomial $g_k(x,a)$ is a **PP** of $\mathbb{F}_q$ if and only if $\gcd(k, q^2-1) = 1$.

In this section we have endeavoured to list the major known classes of **PP**s, but note that we have not attempted an exhaustive survey. Other classes of polynomials have also been characterised; for example, see [32] for polynomials of the form $x^h f(x^{\frac{q-1}{d}})$, and [31] for binomials of the form $x^{m+\frac{q-1}{2}} + ax^m$.

1.5 Normalised Permutation Polynomials

Let $q = p^r$ and let $f(x) = \sum_{i=0}^{n} a_i x^i$ be a **PP** of $\mathbb{F}_q$. Note that the set of **PP**s of $\mathbb{F}_q$ is closed under composition, so in particular the polynomial $g(x) = cf(x + b) + d$ is a **PP** of $\mathbb{F}_q$ for all choices of $b, c, d \in \mathbb{F}_q$, $c \neq 0$. Expanding g, we have

$$g(x) = ca_n x^n + c(a_n bn + a_{n-1})x^{n-1} + \cdots + c(a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0) + d.$$

By suitable choices of c and d we can ensure that g is monic and satisfies $g(0) = 0$; that is, if we choose

$$c = a_n^{-1} \text{ and } d = -c(a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0). \tag{1.8}$$

In addition, if $n \not\equiv 0 \bmod p$ then we can remove the x^{n-1} term by setting

$$b = -a_{n-1}/(a_n n). \tag{1.9}$$

This motivates the following definition.

Definition 1.3. A **PP** $f \in \mathbb{F}_q[x]$ is said to be of **normalised form** if f is monic, $f(0) = 0$, and when the degree n of f is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of x^{n-1} is zero.

Remark 1.2. If $p \nmid n$ then any **PP** $f \in \mathbb{F}_q[x]$ of degree n has a unique normalised representative $g \in \mathbb{F}_q[x]$ given by

$$g(x) = cf(x + b) + d,$$

with b, c, d as defined in (1.8) and (1.9). If $p \mid n$ then with the convention $b = 0$ every **PP** $f \in \mathbb{F}_q[x]$ of degree n has a unique normalised representative $h \in \mathbb{F}_q[x]$ given by

$$h(x) = cf(x) + d,$$

with c, d as defined in (1.8). □

If we divide all **PP**s of $\mathbb{F}_q$ into classes based on their unique normalised representatives then we have a partition of the set of **PP**s of $\mathbb{F}_q$. By counting the number of polynomials in each partition we give an enumerative proof of a classical result in number theory known as Wilson's theorem.

If q is a prime power then there are exactly $q!$ **PP**s of $\mathbb{F}_q$ of degree $< q$. We wish to count the number of **PP**s represented by each normalised **PP** $g \in \mathbb{F}_q[x]$. First consider the monomial $g(x) = x$. This is the only normalised **PP** of degree 1 and is the representative of all linear **PP**s of the form

$$cx + d, \text{ where } c, d \in \mathbb{F}_q, c \neq 0.$$

Hence, $g(x) = x$ represents $q(q-1)$ **PP**s. If g is a normalised **PP** with $\deg(g) > 1$ not divisible by p, then g represents the $q^2(q-1)$ **PP**s given by

$$cg(x+b)+d, \text{ where } b, c, d \in \mathbb{F}_q, c \neq 0.$$

If, on the other hand, $\deg(g) > 1$ and p divides $\deg(g)$, then g represents the $q(q-1)$ **PP**s given by

$$cg(x)+d, \text{ where } c, d \in \mathbb{F}_q, c \neq 0.$$

Hence, if k_1 is the number of nonlinear normalised **PP**s with degree prime to p, and k_2 is the number of normalised **PP**s with degree divisible by p, then we have the identity

$$q! = q(q-1)(1 + k_2 + qk_1). \tag{1.10}$$

Using this identity we give the enumerative proof from [6] of the following theorem.

Theorem 1.23. (Wilson's theorem). *If n is a positive integer then the identity*

$$(n-1)! \equiv -1 \; mod \; n$$

holds if and only if n is prime.

Proof. Let p be a prime and consider the set of **PP**s of $\mathbb{F}_p$. By Lemma 1.2 and Corollary 1.7 we may assume that the degrees of all polynomials are less than $p-1$, thus not being multiples of p. By (1.10) we then have $p! = p(p-1)(1+pk)$ for some positive integer k. Dividing by p and reducing mod p we have

$$(p-1)! \equiv -1 \text{ mod } p.$$

On the other hand, if n is composite then $(n-1)! \equiv 0$ mod p for all prime factors p of n, so $(n-1)! \not\equiv -1$ mod n. □

Chapter 2

The Carlitz Conjecture

In an invited address before the Mathematical Association of America in 1966, Professor L. Carlitz presented a conjecture that would motivate almost 30 years of research and significant interest in permutation polynomials. It had been known since 1897 that there exist **PP**s of degree 1, 3 and 5 over infinitely many fields $\mathbb{F}_q$, but excepting fields of even characteristic there exist only finitely many **PP**s of degree 2, 4 or 6 (see Table A.1, Chapter 3 and [6]). Carlitz conjectured that perhaps this behaviour was typical; that is, except for fields of small order there are no **PP**s of even degree over fields of odd characteristic.

Although there was immediate success in some special cases, progress was made slowly over the next three decades until Carlitz's conjecture was finally resolved in the affirmative by Fried, Guralnick and Saxl in 1993. The story does not end there, however, for around the same time as the work of Fried *et al.* two separate generalisations of Carlitz's conjecture were published. The first, due to Wan, was shortly confirmed. However, a second generalisation conjectured by Mullen has been discussed in published literature but until now has remained unresolved. In Section 2.4 we provide a counterexample to Mullen's conjecture, and also point out how recent results imply an altered version of its statement.

The main goal of this chapter is to give a survey of the major results leading to the proofs of the Carlitz conjecture and Wan's generalisation. We also aim to give some of the history of this journey, and disprove the aforementioned conjecture of Mullen. We will see that the proof of Carlitz's conjecture is closely linked with with the notion of *exceptional polynomials*. These polynomials are discussed in Section 2.1 along with their relationship with permutation polynomials. We will also be concerned with the so-called *value set* of a polynomial, defined as follows: if $f \in \mathbb{F}_q[x]$ is a polynomial then the *value set of f*, denoted V_f, is given by

$$V_f = \{f(c) : c \in \mathbb{F}_q[x]\}.$$

Note that f is a permutation polynomial of $\mathbb{F}_q$ if and only if $|V_f| = q$.

2.1 Exceptional Polynomials

Let F be a field and recall that we have unique factorisation in $F[x_1, x_2, ..., x_n]$ into irreducibles.

Definition 2.1. A polynomial $f \in F[x_1, x_2, ..., x_n]$ is called **absolutely irreducible** if it is irreducible over every algebraic extension of F.

Equivalently, $f \in F[x_1, x_2, ..., x_n]$ is absolutely irreducible if it is irreducible over the algebraic closure of F.

Example 2.1. The polynomial $f(x) = x^2 + 1 \in \mathbb{F}_7[x]$ is irreducible, but not absolutely irreducible because it factors as $(x - \sqrt{-1})(x + \sqrt{-1})$ over $\mathbb{F}_7(\sqrt{-1}) = \mathbb{F}_{7^2}$. In fact, it is easy to see that a univariate polynomial $f \in \mathbb{F}_q[x]$ is absolutely irreducible if and only if it is a linear polynomial. □

Example 2.2. The polynomial $g(x, y) = x^2 + y^2 \in \mathbb{F}_7[x, y]$ is irreducible, but factors as $g(x, y) = (x + \sqrt{-1}y)(x - \sqrt{-1}y)$ over $\mathbb{F}_7(\sqrt{-1}) = \mathbb{F}_{7^2}$. However, the polynomial $h(x, y) = x^2 - y^3 \in \mathbb{F}_7[x, y]$ is absolutely irreducible. □

We now introduce *exceptional polynomials*, which are closely related with permutation polynomials.

Definition 2.2. A polynomial $f \in \mathbb{F}_q[x]$ of degree $\geqslant 2$ is said to be **exceptional** over $\mathbb{F}_q$ if no irreducible factor of

$$\Phi(x, y) = \frac{f(x) - f(y)}{x - y}$$

in $\mathbb{F}_q[x, y]$ is absolutely irreducible.

Equivalently, f is exceptional if every irreducible factor of $\Phi(x, y)$ becomes reducible over some algebraic extension of $\mathbb{F}_q$.

Exceptional polynomials were first introduced by Davenport and Lewis in [5], where the authors also conjectured the following relationship between exceptional polynomials and permutation polynomials. Although special cases were proved by MaCleur [16] and by Williams [34], first general proof was given by Cohen [1] using deep methods of algebraic number theory.

Theorem 2.1. *Every exceptional polynomial over $\mathbb{F}_q$ is a permutation polynomial of $\mathbb{F}_q$.*

In [30], D. Wan shows that Theorem 2.1 is a consequence of the following result, which states that any polynomial producing sufficiently many distinct elements is a **PP**. Wan proves this theorem by way of a p-adic lifting lemma, but we present here the more elementary proof from [23] based on elementary symmetric polynomials.

Recall the following about symmetric polynomials. If R is a ring then a polynomial $f \in R[x_1, ..., x_n]$ is called *symmetric* if $f(x_{i_1}, ..., x_{i_n}) = f(x_1, ..., x_n)$ for any permutation $i_1, ..., i_n$ of the integers $1, ..., n$. If z is an indeterminate over $R[x_1, ..., x_n]$ then the k^{th} *elementary symmetric polynomial* s_k is defined by

$$\prod_{i=1}^{n}(z - x_i) = \sum_{k=0}^{n}(-1)^k s_k z^{n-k}.$$

That is, $s_0 = 1$ and

$$s_k(x_1, ..., x_n) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant n} x_{i_1} \cdots x_{i_k} \text{ for all } 1 \leqslant k \leqslant n.$$

The *fundamental theorem on symmetric polynomials* states that every symmetric polynomial $f(x_1, ..., x_n)$ is a polynomial in $s_1(x_1, .., x_n), ..., s_n(x_1, .., x_n)$.

If $R = \mathbb{F}_q$ is a finite field then it is easy to see that $\prod_{i=1}^{q}(x - c_i) = x^q - x$ if and only if $\{c_1, ..., c_q\} = \mathbb{F}_q$. Hence, if $\{c_1, ..., c_q\} = \mathbb{F}_q$ then we have $s_k(c_1, c_2, ..., c_q) = 0$ for all $1 \leqslant k \leqslant q - 2$. Also note the identity

$$s_k(x, x, ..., x) = \sum_{1 \leqslant i_1 < \cdots < i_k \leqslant q} x^k = \binom{q}{k} x^k = 0 \text{ for all } 1 \leqslant k \leqslant q - 1.$$

Theorem 2.2. (Wan). *Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of positive degree n. If $f(x)$ is not a* **PP** *of $\mathbb{F}_q$, then*

$$|V_f| \leqslant q - \left\lceil \frac{q-1}{n} \right\rceil,$$

where $\lceil m \rceil$ denotes the least integer $\geqslant m$.

Proof. If $n \geqslant q$ then $\left\lceil \frac{q-1}{n} \right\rceil = 1$ and the assertion holds trivially, so assume that $1 \leqslant n \leqslant q - 1$. Then $|V_f| \geqslant 2$, for otherwise f is constant on all values of $\mathbb{F}_q$ in contradiction to Lemma 1.1.

Let $\mathbb{F}_q = \{c_1, ..., c_q\}$ and let s_k represent the k^{th} elementary symmetric polynomial of the values of $f(x)$, that is,

$$\prod_{i=1}^{q}(x - f(c_i)) = \sum_{k=0}^{q}(-1)^k s_k x^{q-k}.$$

Let u be the least positive integer k such that $s_k \neq 0$ if such k exists; otherwise let $u = \infty$.

Suppose that k is such that $0 < kn < q - 1$ and consider the symmetric polynomial $s_k(f(x_1), f(x_2), ..., f(x_q))$. This polynomial has degree at most $kn <$

$q-1$, so by the fundamental theorem on symmetric polynomials it is a polynomial in $s_1(x_1,...,x_q),...,s_{q-2}(x_1,...,x_q)$. Hence, $s_k(f(c_1),...,f(c_q))$ is a polynomial in $s_1(c_1,...,c_q),...,s_{q-2}(c_1,...,c_q)$, all of which are zero. The constant term is $s_k(f(0),...,f(0))=0$. Hence,

$$u \geqslant (q-1)/n. \tag{2.1}$$

Consider the polynomial

$$g(x) = x^q - x - \prod_{i=1}^{q}(x - f(c_i)).$$

Since $\deg\left(x^q - \prod_{i=1}^{q}(x-f(c_i))\right) = q-u$ we have $\deg(g) \leqslant q-u$. Now $g(x)=0$ if and only if $\prod_{i=1}^{q}(x-c_i) = x^q - x$, which is equivalent to f being a **PP**. Hence, if f is not a **PP** then $g(x) \neq 0$. But then $f(c_i)$ is a root of g for all $1 \leqslant i \leqslant q$, so

$$|V_f| \leqslant \deg(g) \leqslant q-u. \tag{2.2}$$

Combining (2.1) and (2.2) we have

$$|V_f| \leqslant q - \left\lceil \frac{q-1}{n} \right\rceil.$$

□

Note that Theorem 2.2 is the precisely the statement given in Theorem 1.12 (5). For Wan's proof that Theorem 2.2 implies Theorem 2.1, see [30, Theorem 5.1].

It is true that all exceptional polynomials are **PP**s, so the converse question naturally arises: are all **PP**s exceptional? The following example shows that this is not the case.

Example 2.3. Let $q=p^r$, $a \in \mathbb{F}_q$, and consider the polynomial

$$f(x) = x^p + a \in \mathbb{F}_q[x]. \tag{2.3}$$

Then f is a **PP** by Theorem 1.15, but we have

$$\Phi(x,y) = \frac{x^p - y^p}{x-y} = \frac{(x-y)^p}{x-y} = (x-y)^{p-1}.$$

All irreducible factors Φ are linear, thus being irreducible over every algebraic extension of $\mathbb{F}_q$. Hence, f is not exceptional. □

The polynomial in (2.3) is a permutation polynomial of $\mathbb{F}_{p^r}$ for all positive integers r. Hence, there exist examples of non-exceptional **PP**s over fields of arbitrarily large order. However, such examples only arise for polynomials that are *not separable*. We will see that excluding these troublesome polynomials it is true that all

PPs are exceptional - provided that q is sufficiently large compared to the degree of the polynomial.

Note that for any $f \in \mathbb{F}_q[x]$ there exists a unique integer $t \geqslant 0$ and a polynomial $g \in \mathbb{F}_q[x]$ such that $f(x) = g(x^{p^t})$, but $f(x) \neq h(x^{p^{t+1}})$ for any $h \in \mathbb{F}_q[x]$. Then $t > 0$ if and only if $f'(x) = 0$. This motivates the following definition.

Definition 2.3. A polynomial $f \in \mathbb{F}_q[x]$ is called **separable** if $f'(x) \neq 0$.

We remark that in other areas of mathematics there exist different definitions of separable polynomials, but in the study of permutation polynomials the above definition is standard (see for example [28, 25, 2, 3]).

Note that if $f(x)$ is not separable then we can write $f(x) = g(x^{p^t})$, where $t > 0$ and $g \in \mathbb{F}_q[x]$ is separable. Then f is a **PP** if and only if g a **PP**, so in most cases we can assume without loss that polynomials are separable (otherwise we could replace f with g).

If we assume separability then it is true that, apart from fields of small order, all **PP**s are exceptional polynomials. The following result was proved by Wan [27] using a powerful theorem of Lang and Weil on the number of rational points of an algebraic curve over a finite field.

Theorem 2.3. *There exists a sequence $c_1, c_2, \ldots$ of integers such that for any separable polynomial $f \in \mathbb{F}_q[x]$ of degree n we have: if $q \geqslant c_n$ and f is a* **PP** *then f is exceptional over $\mathbb{F}_q$.*

We note that Theorem 2.3 had already been proved by Hayes [10] for polynomials satisfying $\gcd(n, q) = 1$. The special case of Hayes' theorem when q is prime was established by Davenport and Lewis [5]; quantitative versions were given by Bombieri and Davenport [4] and Tietäväinen [22].

Although versions of Theorem 2.3 had been known for over 20 years, in 1991 von zur Gathen [25] proved the following version with the explicit sequence $c_n = n^4$. In the language of the previous discussion this quantifies what is meant by a field of 'small order'. As in the work of Hayes and Wan a central ingredient of von zur Gathen's proof is the Lang and Weil theorem. This result ultimately allows the Carlitz conjecture to be stated quantitatively.

Theorem 2.4. *Let $f \in \mathbb{F}_q[x]$ be separable of degree n. If $q \geqslant n^4$ and f is a* **PP***, then f is exceptional.*

In light of Theorem 2.4 we have the following results on the *non existence* of **PP**s of $\mathbb{F}_q$ of certain degrees n. See [15, Ch. 7] for proofs of their non-quantitative analogues; the bound $q \geqslant n^4$ comes from Theorem 2.4, see [25, Corollary 3].

Theorem 2.5. *Let $n \geqslant 1$ and suppose that $q \geqslant n^4$. If $\gcd(n, q) = 1$ and $\mathbb{F}_q$ contains an n^{th} root of unity different from 1 then there is no* **PP** *of $\mathbb{F}_q$ of degree n.*

Corollary 2.6. *Suppose that n is positive and even, $q \geqslant n^4$ and $\gcd(n, q) = 1$. Then there is no* **PP** *of $\mathbb{F}_q$ of degree n.*

Proof. Let $\zeta = -1$ in Theorem 2.5. □

Corollary 2.7. *Suppose that $q \geqslant n^4$ and $\gcd(n, q) = 1$. Then there exists a* **PP** *of $\mathbb{F}_q$ of degree n if and only if $\gcd(n, q-1) = 1$.*

Proof. If $\gcd(n, q-1) = 1$ then the monomial x^n is a **PP** of $\mathbb{F}_q$ by Theorem 1.14. Conversely, suppose that $\gcd(n, q-1) = d > 1$. Since the multiplicative group $\mathbb{F}_q^\times$ is cyclic of order $q-1$ it follows that $g^{(q-1)/d}$ is an n^{th} root of unity different to 1, where g is a primitive element of $\mathbb{F}_q$. □

2.2 A Conjecture of Carlitz

In an invited address before the Mathematics Association of America in 1966, Professor L. Carlitz made the following conjecture:

Proposition 2.8. (Carlitz conjecture). *For every even positive integer n, there is a constant c_n such that for each finite field of odd order $q > c_n$, there does not exist a* **PP** *of $\mathbb{F}_q$ of degree n.*

This proposition was the motivation for many papers and generated much interest over the following three decades. A chronology of the major results leading to the proof of Proposition 2.8 is given below. Carlitz' conjecture was finally resolved in the affirmative by Fried, Guralnick and Saxl in 1993. They used the classification of finite simple groups to prove, in particular, the following theorem.

Theorem 2.9. (Fried *et al.*). *If q is odd then every exceptional polynomial over $\mathbb{F}_q$ has odd degree.*

In light of Theorem 2.4 this confirms the Carlitz conjecture. We state this as a theorem.

Theorem 2.10. *Let n be a positive even integer and suppose that $q \geqslant n^4$ is odd. Then there does not exist a* **PP** *of $\mathbb{F}_q$ of degree n.*

Proof. Let n be an even positive integer and let $q = p^r \geqslant n^4$ be odd. Suppose that $f \in \mathbb{F}_q[x]$ has degree n. We may assume that f is separable. For otherwise, write $f(x) = g(x^{p^t})$, where $g'(x) \neq 0$ and t is a positive integer. Then $g \in \mathbb{F}_q[x]$ is separable of even degree $m = n/p^t$, and $q \geqslant m^4 = n^4/p^{4t}$. Moreover, f is a **PP** of $\mathbb{F}_q$ if and only if g is, so we may replace f by g and n by m. Hence, assume that f is separable. If f is a **PP** then it is exceptional by Theorem 2.4, but then n is odd by Theorem 2.9, a contradiction. □

The following is a timeline of the major results leading to the proof of Theorem 2.10.

1897 Dickson's list (Chapter 3, Table A.1,[6]) shows that there are only finitely many fields $\mathbb{F}_q$ of odd characteristic containing **PP**s of degree $n = 2, 4, 6$.

1966 Carlitz presents his conjecture during an address to the MAA.

1967 Hayes [10] proves the conjecture for $n = 8, 10$ and the general case case $p \nmid n$.

1973 Lausch and Nobauer [12, p. 202] prove the conjecture for $n = 2^m$.

1987 Wan [27] proves the conjecture for $n = 12, 14$ and states an equivalent version in terms of exceptional polynomials.

1988 Lidl and Mullen [14, P9] feature the Carlitz conjecture as an unsolved problem.

1990 Wan [28] proves the conjecture for $n = 2r$, where r is an odd prime.

1991 Independently to Wan, and almost at the same time, Cohen [2] proves the case $n = 2r$, r an odd prime. In addition, he proves the conjecture for all $n < 1000$.

1991 von zur Gathen [25] proves Theorem 2.4, allowing the Carlitz conjecture to be stated quantitatively.

1993 Carlitz's conjecture is proven in general by Fried, Guralnick and Saxl [9].

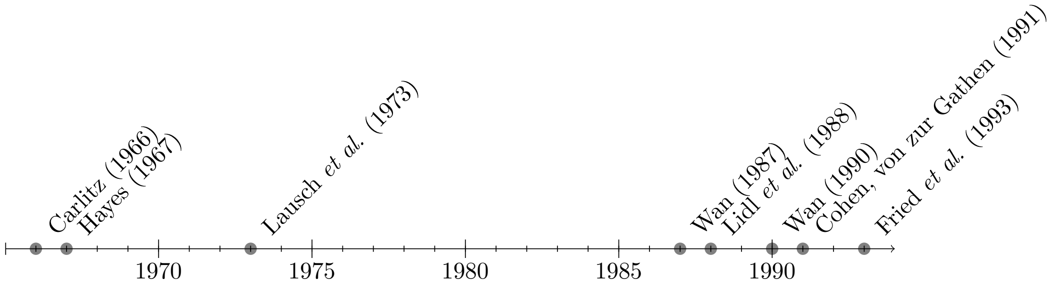

Figure 2.1: *A timeline of major results leading to the proof of the Carlitz conjecture.*

2.3 Wan's Generalisation

Coinciding with the time that Fried *et al.* proved Carlitz's original conjecture, in 1993 Wan proposed the following generalisation [29].

Proposition 2.11. (Carlitz-Wan conjecture). *Let $q > n^4$. If $\gcd(n, q-1) > 1$, then there are no* **PP***s of degree n over $\mathbb{F}_q$.*

Recall that if $\gcd(n, q-1) = 1$ then there exist **PP**s of degree n (for example the monomial x^n). Proposition 2.11 can be interpreted as a partial converse of this statement; that is, if $q > n^4$ then there exist **PP**s of degree n if and only if $\gcd(n, q-1) = 1$. In the special case that n is even and q is odd, Proposition 2.11 reduces to the Carlitz conjecture (Proposition 2.8).

The work by Fried *et al.* in [9], which proved Carlitz's original conjecture, also proved the Carlitz-Wan conjecture for fields of characteristic $p > 3$. The remaining special cases did not remain unresolved for long, for the following theorem by Lenstra implies Proposition 2.11 in full generality. See [3] for a discussion of Lenstra's proof and an elementary version.

Theorem 2.12. (Lenstra). *Suppose* $\gcd(n, q-1) > 1$. *Then there is no exceptional polynomial of degree* n *over* $\mathbb{F}_q$.

We state Wan's generalisation of the Carlitz conjecture as a theorem.

Theorem 2.13. *Let* $q > n^4$. *If* $\gcd(n, q-1) > 1$, *then there are no* **PP***s of degree* n *over* $\mathbb{F}_q$.

Proof. Note that as in the proof of Theorem 2.10 we may assume without loss that all polynomials are separable. The result follows from Theorem 2.12 and Theorem 2.4. □

2.4 On a Conjecture of Mullen

The following generalisation of Carlitz's conjecture by Mullen appeared in [17] and is discussed in [30, 23, 18, 29]. Until now it is an unresolved problem in published literature.

Based on computer calculations, Mullen proposed that if n is even and q is odd and sufficiently large then no polynomial is "close" to being a **PP**.

Conjecture 2.14. (Mullen). *If* n *is even,* q *is odd with* $q > n(n-2)$ *and* $f \in \mathbb{F}_q[x]$ *has degree* n*, then*

$$|V_f| \leqslant q - \left\lceil \frac{q-1}{n} \right\rceil .$$

In light of Theorem 2.2 and Theorem 2.10 (both appearing after Mullen's conjecture) we know this to be true for all $q \geqslant n^4$. We present a counterexample to Mullen's conjecture as stated. Let a be an arbitrary nonzero element of $\mathbb{F}_{3^3}$ and consider the polynomial

$$f(x) = x^6 + ax^5 - a^4x^2 \in \mathbb{F}_{3^3}[x].$$

Then f is a **PP** of $\mathbb{F}_{3^3}$, as proved in Section 3.4.2 and [6]. This contradicts Conjecture 2.14, because $27 = q > n(n-2) = 24$, but

$$| V_f |= 27 \nleqslant 22 = q - \left\lceil \frac{q-1}{n} \right\rceil .$$

Armed with results published after Mullen's conjecture (Theorem 2.2 and Theorem 2.13) we can give the following generalisation of Conjecture 2.14, although the bound on q is considerably weakened. In the special case that n is even and q is odd, this reduces (albeit with a looser bound) to Mullen's conjecture.

Theorem 2.15. *If* $\gcd(n, q-1) > 1$ *with* $q > n^4$ *and* $f \in \mathbb{F}_q[x]$ *has degree* n*, then*

$$|V_f| \leqslant q - \left\lceil \frac{q-1}{n} \right\rceil .$$

Proof. Theorem 2.13 and Theorem 2.2. □

It would be interesting if future research could further reduce the bound in Theorem 2.15; by the above discussion the true bound lies between $n(n-2)$ and n^4.

Chapter 3

Permutation Polynomials of Degree 6

In 1897 Leonard Eugene Dickson [6] claimed to give, aside from degree 6 polynomials in even characteristic, a *complete list of all reduced quantics of degree* $\leqslant 6$ *which are suitable to represent substitutions.* In modern parlance this is a claim to a complete list of normalised permutation polynomials (compare [6, §16] to Definition 1.3). Historically, Dickson's claim has been largely accepted in literature [15, 10, 27, 28, 13], however in more recent times some doubts have been cast on this assertion. Though his classification of polynomials of degree less than 6 is still trusted, some authors have questioned the completeness of his characterisation of the degree 6, odd characteristic case. Indeed, [8] refers to this as a 'partial list'.

The main problem with verifying Dickson's claim is that his published proof in [6] is very difficult to follow. To his credit, the author did a remarkable job in deriving and solving the necessary sets of long, unfriendly equations without so much as a pocket calculator. However, his long and tricky proof is not easily accessible to the modern mathematician for a number of reasons, the main factor being that his language, notation and terminology are somewhat antiquated 115 years later. Furthermore, as is natural for a paper written before modern computing and printing, there are some unhelpful typographical errors and inconsistent notations. For these reasons, it has not been easy for the modern mathematician to verify Dickson's claim to a complete classification.

In this chapter we recreate in full detail the classical result of Dickson by deriving the full characterisation of degree 6 permutation polynomials in odd characteristic. The aim of this chapter is to finally put to rest the classification problem for permutation polynomials of degree $\leqslant 6$. Though our general ideas and methods are essentially the same as in [6], we have not attempted to recreate Dickson's proof step-by-step. Indeed, in many ways our proofs are different to those presented in [6]. We deliberately give most details, for we feel that many of the rearrangements and tricks used in solving sets of equations are nonobvious. Our goal is a proof that can be easily followed in full detail by those who are unconvinced by Dickson's claim of a complete characterisation. Hopefully the arguments presented are more easily accessible to the modern mathematician than those in the original paper.

Somewhat surprisingly, we find that the list given in [6] is, albeit with minor errors, indeed a full classification. We are, however, able to improve Dickson's list in several ways. In [6], we note that not all *normalised* permutation polynomials of degree 6 in characteristic 3 are listed. Instead, some of Dickson's polynomials have been reduced further than specified in Definition 1.3. We are able to rectify this, and we suggest that confusion over this point is perhaps the reason that Dickson's list has been recently questioned. Furthermore, we clear up some errors in the list, and give a much cleaner parametrisation of one of the entries. In light of a very recent paper by Li *et al.* [13], which lists all degree 6 and 7 **PP**s over fields of characteristic 2, this completes the classification problem of **PP**s of degree $\leqslant 6$.

3.1 Some General Results

3.1.1 The Multinomial Theorem Modulo p

We begin by defining multinomial coefficients, which the next theorem shows are analogous to the well-known binomial coefficients.

Definition 3.1. If $t, n, k_1, ..., k_n$ are nonnegative integers with $k_1 + \cdots + k_n = t$ and $n \geqslant 2$, then define the **multinomial coefficient** $\binom{t}{k_1, k_2, ..., k_n}$ to be

$$\binom{t}{k_1, k_2, ..., k_n} = \frac{t!}{k_1! k_2! \cdots k_n!}.$$

The following theorem is known as the multinomial theorem.

Theorem 3.1. *We have the following expansion:*

$$(x_1 + \cdots + x_n)^t = \sum_{\substack{k_1 + \cdots + k_n = t \\ k_1 \geqslant 0, \cdots, k_n \geqslant 0}} \binom{t}{k_1, ..., k_n} x_1^{k_1} \cdots x_n^{k_n}.$$

The following is the multinomial analogue of a classical theorem of Lucas. Its proof can be found in [6, §14-15].

Theorem 3.2. *Let p be a prime and $k_1, k_2, ..., k_n, t$ be nonnegative integers such that $k_1 + k_2 + \cdots + k_n = t$. Suppose that we have the following p-adic expansions:*

$$k_i = b_{i0} + b_{i1}p + b_{i2}p^2 + \cdots + b_{is}p^s \text{ for all } 1 \leqslant i \leqslant n,$$
$$t = c_0 + c_1 p + c_2 p^2 + \cdots + c_s p^s,$$

where $0 \leqslant c_j, b_{ij} \leqslant p-1$ *for all* $0 \leqslant j \leqslant s$ *and* $1 \leqslant i \leqslant n$. *Then*

$$\binom{t}{k_1, k_2, ..., k_n} \not\equiv 0 \textit{ mod } p \textit{ if and only if } \sum_{i=1}^{n} b_{ij} = c_j \textit{ for all } 0 \leqslant j \leqslant s.$$

If $\binom{t}{k_1,k_2,...,k_n} \not\equiv 0$ *mod* p *then we have*

$$\binom{t}{k_1, k_2, ..., k_n} \equiv \binom{c_0}{b_{10}, b_{20}, ..., b_{n0}} \cdots \binom{c_s}{b_{1s}, b_{2s}, ..., b_{ns}} \textit{ mod } p.$$

3.1.2 A General Restriction on Coefficients

The following theorem shows that any normalised **PP** of degree n of $\mathbb{F}_q$, where $q \equiv -1 \bmod n$, has no x^{n-2} term.

Theorem 3.3. *Let*

$$f(x) = x^n + a_{n-2}x^{n-2} + \cdots + a_1 x \in \mathbb{F}_q[x]$$

be a normalised **PP** *of* $\mathbb{F}_q$, *where* $3 \leqslant n \leqslant q-2$ *and* $q = p^r \equiv -1$ *mod* n. *Then* $a_{n-2} = 0$.

Proof. Note that $p^r \equiv -1 \bmod n$ implies that $p \nmid n$, so f is indeed the general form for a normalised **PP** of degree n (Definition 1.3).

Write $q = nm - 1$; then it is clear that $m = (q+1)/n \not\equiv 0 \bmod p$. We also have

$$1 < m = \frac{q+1}{n} \leqslant q - 2,$$

because $1 < (q+1)/n$ is equivalent to $q > n-1$ and $(q+1)/n \leqslant q-2$ is equivalent to $q \geqslant (2n+1)/(n-1)$, and both of these conditions hold under the assumption $3 \leqslant n \leqslant q-2$. Hence, by Theorem 1.5, the reduction of $f(x)^m$ modulo $x^q - x$ has degree $\leqslant q-2$.

To find the coefficient of x^{q-1} in $f(x)^m \bmod (x^q - x)$ we are interested in coefficients of terms of the form $x^{i(q-1)}$ in the expansion of $f(x)^m$. But $\deg(f(x)^m) = nm$, and we have, since $nm \geqslant 6$,

$$q - 1 = nm - 2 < nm < 2nm - 4 = 2(q-1).$$

So there are no terms of the form $x^{i(q-1)}$ for $i \geqslant 2$.

We use the multinomial theorem to find the coefficient of $x^{q-1} = x^{nm-2}$. By Theorem 3.1 we have

$$f(x)^m = \sum_{\substack{k_1+\cdots+k_{n-2} \\ +k_n = m}} \binom{m}{k_1, ..., k_{n-2}, k_n} a_1^{k_1} \cdots a_{n-2}^{k_{n-2}} \cdot x^{k_1 + \cdots + (n-2)k_{n-2} + n \cdot k_n}.$$

To find the coefficient of $x^{q-1} = x^{nm-2}$ we must find all solutions over the nonnegative integers of the following system.

$$\begin{cases} k_1 + \cdots + k_{n-2} + k_n = m, & (a) \\ k_1 + 2k_2 + \cdots + (n-2)k_{n-2} + n \cdot k_n = nm - 2. & (b) \end{cases}$$

We observe that we must have $k_n = m - 1$. For if $k_n = m$ then the *LHS* of (b) is immediately too large. On the other hand, if $k_n < m - 1$ then the *LHS* of (b) is too small, for even if $k_{n-2} = m - k_n$ we have

$$(n-2)(m-k_n) + n \cdot k_n = (n-2)m + 2k_n < nm - 2.$$

So we must have $k_n = m - 1$, in which case the system reduces to

$$\begin{cases} k_1 + \cdots + k_{n-2} = 1, & (a) \\ k_1 + 2k_2 + \cdots (n-2)k_{n-2} = n - 2. & (b) \end{cases}$$

The only solution is

$$k_1 = \cdots = k_{n-3} = 0, k_{n-2} = 1, k_n = m - 1.$$

Thus the coefficient of x^{q-1} in $f(x)^m$ mod $(x^q - x)$ is $\frac{m!}{(m-1)!}a_{n-2}$, so we have

$$m \cdot a_{n-2} = 0.$$

Since we observed that $m \not\equiv 0$ mod p we must have $a_{n-2} = 0$. □

3.2 Restrictions on p and q

In this section we determine necessary restrictions on p and $q = p^r$ for **PP**s of degree 6 to exist in $\mathbb{F}_q[x]$. We first note that the affirmatively resolved Carlitz-Wan conjecture (Theorem 2.13) gives us the upper bound $q \leqslant 6^4$. In fact we won't assume this theorem because Dickson's original classification in [6] claims to show this purely from Hermite's criterion. Indeed, we will find that all degree 6 **PP**s of $\mathbb{F}_q$ satisfy $q \leqslant 27$. An interesting historical note is that Dickson's characterisation of degree 6 **PP**s was used in partial proofs of the Carlitz conjecture [10, 27, 28] before the general proof was found by Fried *et al.* in [9].

Suppose that $f(x)$ is a degree 6 **PP** of $\mathbb{F}_q$, where q is odd. To apply Hermite's criterion we will need to treat separately the different residue classes of q modulo 6, for the term of degree $q-1$ in the expansion of $f(x)^t$ depends on the residue class of q. If $q = p^r$ then we write q in the form

$$q = 6m + \mu, \text{ with } 0 \leqslant \mu \leqslant 5.$$

Now since q is odd by assumption it is impossible that μ is even. Also, the case $\mu = 1$ is impossible by Corollary 1.8. So the two cases are $q = 6m+3$, in which case $p = 3$, and $q = 6m+5$, in which case $p \equiv 5 \bmod 3$ and r is odd, as the following lemma shows.

Lemma 3.4. *We have $p^r \equiv 5$ mod 6 if and only if $p \equiv 5$ mod 6 and r is odd.*

Proof. Since $5 \equiv -1 \bmod 6$ the reverse implication is trivial. Suppose that $p^r \equiv 5 \bmod 6$. Then $p^r \equiv 1 \bmod 2$ and $p^r \equiv 2 \bmod 3$. These conditions imply, respectively, that $p \equiv 1 \bmod 2$, and $p \equiv 2 \bmod 3$ with r odd. Hence, $p \equiv 5 \bmod 6$ and r is odd. □

3.3 Degree 6 PPs of $\mathbb{F}_{6m+5}$

The aim of this section is to classify all normalised **PP**s of degree 6 over finite fields of the form $\mathbb{F}_{6m+5}$. By Definition 1.3 and Theorem 3.3 such a polynomial has the general form

$$f(x) = x^6 + a_3x^3 + a_2x^2 + a_1x. \tag{3.1}$$

We remark that we are only interested in finite fields of order $q \geqslant 11$, because any degree 6 **PP** of $\mathbb{F}_5$ can be reduced mod $x^5 - x$ to a polynomial of degree $\leqslant 3$ (by Lemma 1.2 and Corollary 1.7). Thus, no **PP** of $\mathbb{F}_5$ is a true degree 6 polynomial.

For any **PP** $f(x)$ of the form (3.1) we now use Hermite's criterion to derive a set of necessary equations in the coefficients a_1, a_3, a_3. Since $\deg(f(x)^m) = 6m = q-5$ and $\deg(f(x)^{m+1}) = 6m+6 = q+1$, we observe that $f(x)^{m+1}$ is the first power of $f(x)$ with degree $\geqslant q-1$. Hence $m+1$ is the first useful power to apply in Hermite's criterion. However, Theorem 3.3 ensures that the polynomial (3.1) always satisfies the power $f(x)^{m+1}$, so we begin by considering the next useful power, namely $f(x)^{m+2}$. We will require the following inequality

$$1 \leqslant m \leqslant q - 10 \text{ for all } q \geqslant 11. \tag{3.2}$$

Lemma 3.5. *Let*

$$f(x) = x^6 + a_3x^3 + a_2x^2 + a_1x \in \mathbb{F}_q[x]$$

be a **PP** *of $\mathbb{F}_q$, where $q = p^r = 6m+5$. If $q \geqslant 11$ then*

$$a_2^2 + 2a_1a_3 = 0. \tag{3.3}$$

If $q > 11$ then

$$36a_1^2a_2 - 15a_2^2a_3^2 - 10a_1a_3^3 = 0. \tag{3.4}$$

If $q > 17$ then

$$72a_1^4 - 12a_2^5 - 240a_1a_2^3a_3 - 360a_1^2a_2a_3^2 + 55a_2^2a_3^4 + 22a_1a_3^5 = 0. \tag{3.5}$$

Proof. Note that $m+\frac{5-p}{6}$ and $m+\left(\frac{5-p}{6}+p\right)$ are consecutive multiples of p. Since $p \geqslant 5$ this implies that there are no multiples of p lying strictly between m and $m+6$; in particular, the integers $m+2, m+3$ and $m+4$ are not divisible by p. We also have, by (3.2),

$$3 \leqslant m+2, m+3, m+4 \leqslant q-6.$$

So by Theorem 1.5, the reductions of $f(x)^{m+2}, f(x)^{m+3}, f(x)^{m+4}$ modulo $x^q - x$ have degree $\leqslant q-2$.

First consider the expansion of $f(x)^{m+2}$. We are interested in the coefficient of x^{q-1} in $f(x)^{m+2}$ mod $(x^q - x)$, which means we must find coefficients of the terms $x^{i(q-1)}$ in $f(x)^{m+2}$. But the highest power of x in $f(x)^{m+2}$ is $6(m+2) = q+7$, so if there were any terms in $x^{i(q-1)}$ with $i \geqslant 2$ then we would have

$$q+7 \geqslant 2(q-1),$$

which is equivalent to $q \leqslant 9$. Since $q \geqslant 11$ there are no such terms, so we only need to consider the coefficient of $x^{q-1} = x^{6m+4}$.

By Theorem 3.1 we have

$$f(x)^{m+2} = \sum_{\substack{k_1+k_2+k_3\\ +k_6=m+2}} \binom{m+2}{k_1, k_2, k_3, k_6} a_1^{k_1} a_2^{k_2} a_3^{k_3} \cdot x^{k_1+2k_2+3k_3+6k_6}.$$

We must find all solutions over the nonnegative integers of the following system.

$$\begin{cases} k_1+k_2+k_3+k_6 = m+2, & (a)\\ k_1+2k_2+3k_3+6k_6 = 6m+4. & (b)\end{cases}$$

We give an outline of this routine task. First note that $k_6 \leqslant m$, for otherwise $k_6 \geqslant m+1$, in which case $6k_6 \geqslant 6m+6$ in contradiction to (b). We must also have $k_6 \geqslant m$, for otherwise $k_6 \leqslant m-1$, in which case *LHS* of (b) can be at most, with $k_3 = m+2-k_6$,

$$3(m+2-k_6)+6k_6 = 3m+6+3k_6 \leqslant 6m+3.$$

Hence $k_6 = m$, and the system reduces to

$$\begin{cases} k_1+k_2+k_3 = 2, & (a)\\ k_1+2k_2+3k_3 = 4, & (b)\end{cases}$$

which is easily solvable over the finite domain of possibilities. The solutions are

k_1	k_2	k_3	k_6
0	2	0	m
1	0	1	m

Hence, the coefficient of x^{q-1} in $f(x)^{m+2} \bmod (x^q - x)$ is

$$\frac{(m+2)!}{2!m!}a_2^2 + \frac{(m+2)!}{m!}a_1a_3 = \frac{(m+2)(m+1)}{2}a_2^2 + (m+2)(m+1)a_1a_3.$$

Equating this to zero (by Theorem 1.5) and dividing by $(m+2)(m+1)/2 \neq 0$ we have

$$a_2^2 + 2a_1a_3 = 0.$$

Now suppose that $q > 11$, so that $q \geqslant 17$ since $q \equiv 5 \bmod 6$. By a similar process we must find the coefficient of x^{q-1} in $f(x)^{m+3} \bmod (x^q - x)$. As before, we note that there are no terms in $f(x)^{m+3}$ of the form $x^{i(q-1)}, i \geqslant 2$. For the highest power of x in $f(x)^{m+3}$ is $6m + 18 = q + 13$, and $2(q-1) > q + 13$ for all $q > 15$. So we only need to find the coefficient of x^{q-1}.

To find the coefficient of $x^{q-1} = x^{6m+4}$ in $f(x)^{m+3}$ we must solve the following system

$$\begin{cases} k_1 + k_2 + k_3 + k_6 = m + 3, & (a) \\ k_1 + 2k_2 + 3k_3 + 6k_6 = 6m + 4. & (b) \end{cases}$$

By similar reasoning to the previous case we deduce that $m - 1 \leqslant k_6 \leqslant m$, and in both cases the system is easily solvable. The solutions are

k_1	k_2	k_3	k_6
2	1	0	m
0	2	2	$m-1$
1	0	3	$m-1$

Hence, by Theorem 1.5, we have the identity

$$\begin{aligned} 0 &= \frac{(m+3)!}{2 \cdot m!}a_1^2a_2 + \frac{(m+3)!}{4(m-1)!}a_2^2a_3^2 + \frac{(m+3)!}{6(m-1)!}a_1a_3^3 \\ &= \frac{(m+3)(m+2)(m+1)}{12}\left[6a_1^2a_2 + m(3a_2^2a_3^2 + 2a_1a_3^3)\right] \end{aligned}$$

We may divide by $(m+3)(m+2)(m+1)/12 \neq 0$ and substitute $m = -5/6$ (since $m = (p^r - 5)/6$). Simplifying, we have

$$36a_1^2a_2 - 15a_2^2a_3^2 - 10a_1a_3^3 = 0.$$

Finally, suppose that $q > 17$ and consider the coefficient of x^{q-1} in $f(x)^{m+4} \bmod (x^q - x)$. As before we deduce that there are no terms of the form $x^{i(q-1)}, i \geqslant 2$, so we only need to consider the coefficient of x^{q-1} in $f(x)^{m+4}$. To find this coefficient we must solve

$$\begin{cases} k_1 + k_2 + k_3 + k_6 = m + 4, & (a) \\ k_1 + 2k_2 + 3k_3 + 6k_6 = 6m + 4. & (b) \end{cases} \tag{3.6}$$

We have $m-2 \leqslant k_6 \leqslant m$, and the solutions are

k_1	k_2	k_3	k_6
4	0	0	m
0	5	0	$m-1$
1	3	1	$m-1$
2	1	2	$m-1$
0	2	4	$m-2$
1	0	5	$m-2$

We must perhaps address the fact that $k_6 = m-2$ is not a valid solution to (3.6) if $m < 2$. However, since $q > 17$ and $m = (q-5)/6$ we have in fact that $m > 2$, so that the given solutions are valid. Hence we have the identity

$$\frac{(m+4)!}{m!}\frac{a_1^4}{4!} + \frac{(m+4)!}{(m-1)!}\left(\frac{a_2^5}{5!} + \frac{a_1a_2^3a_3}{6} + \frac{a_1^2a_2a_3^2}{4}\right) + \frac{(m+4)!}{(m-2)!}\left(\frac{a_2^2a_3^4}{2\cdot 4!} + \frac{a_1a_3^5}{5!}\right) = 0.$$

Dividing by $(m+4)(m+3)(m+2)(m+1) \neq 0$, substituting $m = -5/6$ and simplifying we have

$$\frac{a_1^4}{4!} - \frac{a_2^5}{6\cdot 4!} - \frac{5a_1a_2^3a_3}{36} - \frac{5a_1^2a_2a_3^2}{24} + \frac{55a_2^2a_3^4}{72\cdot 4!} + \frac{11a_1a_3^5}{36\cdot 4!} = 0.$$

Multiplying by $72\cdot 4! = 2^6\cdot 3^3 \neq 0$ we have

$$72a_1^4 - 12a_2^5 - 240a_1a_2^3a_3 - 360a_1^2a_2a_3^2 + 55a_2^2a_3^4 + 22a_1a_3^5 = 0.$$

□

Armed with the equations derived in Lemma 3.5 our next goal is to prove that there are no degree 6 **PP**s of $\mathbb{F}_q$ if $q > 11$. The following important lemma shows that the linear term of a normalised degree 6 **PP** of $\mathbb{F}_q$ is necessarily nonzero.

Lemma 3.6. *Let*

$$f(x) = x^6 + a_3x^3 + a_2x^2 + a_1x \in \mathbb{F}_q[x]$$

be a **PP** *of* $\mathbb{F}_q$*, where* $q = p^r = 6m+5$*. Then* $a_1 \neq 0$*.*

Proof. If $a_1 = 0$ then (3.3) implies that $a_2 = 0$, so that $f(x) = x^6 + a_3x^3$. Consider the quadratic polynomial $g(x) = x^2 + a_3x \in \mathbb{F}_q[x]$. By normalisation $g(x)$ is a **PP** of $\mathbb{F}_q$ if and only if the monomial x^2 is a **PP**, which occurs precisely when $3 \mid q$ (Theorem 1.14). Since $p \neq 3$, $g(x)$ is not a **PP** of $\mathbb{F}_q$, so neither is $g(x^3) = f(x)$. □

We now show that there are no degree **PP**s of $\mathbb{F}_q$ in the special case $q = 17$.

Theorem 3.7. *There are no degree 6* **PP***s of* $\mathbb{F}_{17}$*.*

Proof. Suppose that $f(x)$ is a degree 6 **PP** of $\mathbb{F}_{17}$. By normalisation and (3.1) we may express $f(x)$ in the form

$$f(x) = x^6 + a_3x^3 + a_2x^2 + a_1x.$$

Reducing (3.3) and (3.4) modulo 17, we have

$$\begin{cases} a_2^2 + 2a_1a_3 = 0, & (1) \\ 2a_1^2a_2 + 2a_2^2a_3^2 + 7a_1a_3^2 = 0. & (2). \end{cases}$$

We use Hermite's criterion to derive a third necessary equation in the coefficients of $f(x)$. By Theorem 1.5 the reduction of $f(x)^6$ modulo $x^{17} - x$ has degree $\leqslant 15$. Upon performing this expansion and equating the coefficient of x^{16} to zero we have

$$15a_1^4 + 6a_2 + 6a_2^5 + a_1a_2^3a_3 + 10a_1^2a_2a_3^2 + 15a_2^2a_3^4 + 6a_1a_3^5 = 0. \quad (3)$$

Since $a_1 \neq 0$ (Lemma 3.6) we have by (1) that $a_3 = -a_2^2/(2a_1)$. Substituting this into (2) and (3) and multiplying each by a suitable power of a_1 we get

$$\begin{cases} 2a_1^4a_2 + 6a_2^6 = 0, & (2') \\ 15a_1^8 + 6a_1^4a_2 + 8a_1^4a_2^5 + 5a_2^{10} = 0. & (3') \end{cases}$$

If $a_2 = 0$ then $(3')$ implies that $a_1 = 0$ in contradiction to Lemma 3.6, so we may assume that $a_2 \neq 0$. Dividing $(2')$ by a_2 and simplifying, we have $a_2^5 = 11a_1^4$. Subsitituing this into $(3')$ we get $a_2 = a_1^4$. Hence we have

$$\begin{cases} a_2^5 = 11a_1^4, & (2'') \\ a_2 = a_1^4. & (3''). \end{cases}$$

But dividing $(2'')$ by $(3'')$ gives $a_2^4 = 11$, and 11 has no fourth root in $\mathbb{F}_{17}$, a contradiction. □

We are now able to prove the more general result that there are no degree 6 **PP**s of $\mathbb{F}_q$ when $q > 11$.

Theorem 3.8. *Let $q = 6m + 5 > 11$. Then there are no degree 6* **PP***s of* $\mathbb{F}_q$.

Proof. Let $f(x)$ be a degree 6 **PP** of $\mathbb{F}_q$, where $q = p^r = 6m + 5 > 11$. Since the $q = 17$ case was considered in Theorem 3.7 we may assume that $q > 17$.

Moreover we may assume that f is normalised, so by (3.1) and Lemma 3.5 we have

$$f(x) = x^6 + a_3x^3 + a_2x^2 + a_1x,$$

where

$$\begin{cases} a_2^2 + 2a_1a_3 = 0, & (1) \\ 36a_1^2a_2 - 15a_2^2a_3^2 - 10a_1a_3^3 = 0, & (2) \\ 72a_1^4 - 12a_2^5 - 240a_1a_2^3a_3 - 360a_1^2a_2a_3^2 + 55a_2^2a_3^4 + 22a_1a_3^5 = 0. & (3) \end{cases}$$

Note also that $a_1 \neq 0$ by Lemma 3.6.

If $a_2 = 0$ then $a_3 = 0$ by (1), but then by (3) we have $a_1 = 0$, a contradiction. So we may assume that $a_2 \neq 0$.

Now by (1) we have $a_3 = -a_2^2/(2a_1)$. Substituting this into (2) and (3) and dividing by $a_2 \neq 0$ where necessary, we have

$$\begin{cases} 5a_2^5 = 72a_1^4, & (2') \\ 288a_1^8 + 72a_1^4a_2^5 + 11a_2^{10} = 0. & (3') \end{cases}$$

If $p = 5$ then $(2')$ implies that $a_1 = 0$, a contradiction. If $p \neq 5$ then substituting $a_2^5 = 72a_1^4/5$ into $(3')$ gives

$$\frac{90144}{25}a_1^8 = 0,$$

and since $90144 = 2^5 \cdot 3^2 \cdot 313$ is a product of primes $\not\equiv 5 \bmod 6$, we have $a_1 = 0$, a contradiction. □

Our results so far have reduced the characterisation of degree 6 **PP**s of $\mathbb{F}_{6m+5}$ to the case $6m + 5 = 11$. In contrast to the fields of higher order there do exist degree 6 **PP**s of $\mathbb{F}_{11}$, and the following theorem gives their complete characterisation.

Theorem 3.9. *The following is the complete list of normalised degree 6* **PP***s of* $\mathbb{F}_{11}$*:*

$$\begin{gathered} x^6 \pm 2x, \\ x^6 \pm 4x, \\ x^6 \pm a^2x^3 + ax^2 \pm 5x \ (a \text{ a nonzero square}), \\ x^6 \pm 4a^2x^3 + ax^2 \pm 4x \ (a \text{ a nonsquare}). \end{gathered}$$

Proof. By (3.1), let

$$f(x) = x^6 + a_3x^3 + a_2x^2 + a_1x \in \mathbb{F}_{11}[x]$$

be a normalised **PP** of $\mathbb{F}_{11}$. Then by Theorem 1.5 the reductions of $f(x)^3$, $f(x)^4$ and $f(x)^5$ modulo $x^{11} - x$ must have degree $\leqslant 10$. Performing these expansions (routine calculations omitted) and equating the coefficient of x^{10} to zero in each case, we get the necessary conditions

$$\begin{cases} a_2^2 + 2a_1a_3 = 0, & (1) \\ 4a_2 + a_1^2a_2 + 6a_2^2a_3^2 + 4a_1a_3^3 = 0, & (2) \\ 1 + 10a_1^2 + 5a_1^4 + a_2^5 + 9a_1a_2^3a_3 + 8a_2a_3^2 + 8a_1^2a_2a_3^2 = 0. & (3) \end{cases}$$

Since $a_1 \neq 0$ (Lemma 3.6), we may express (1) as $a_3 = -a_2^2/(2a_1)$. Substituting this into (2) and (3) and simplifying gives

$$\begin{cases} a_3 = -a_2^2/(2a_1), & (1') \\ 4a_1^2 a_2 + a_1^4 a_2 + a_2^6 = 0, & (2') \\ 2a_1^2 + 9a_1^4 + 10a_1^6 + 4a_2^5 + 8a_1^2 a_2^5 = 0. & (3') \end{cases}$$

If $a_2 = 0$ then $a_3 = 0$ by $(1')$, and $(3')$ reduces to

$$a_1^4 + 2a_1^2 + 9 = 0.$$

By the quadratic formula we then have $a_1^2 = 4$ or 5, so that $a_1 = \pm 2$ or ± 4. Thus we have the following candidates for **PP**s:

$$x^6 \pm 2x, x^6 \pm 4x.$$

If $a_2 \neq 0$ then we may divide $(2')$ by a_2 and rearrange to get $a_2^5 = 10a_1^2(a_1^2 + 4)$. Substituting this into $(3')$ we have

$$a_1^4 + 3a_1^2 + 4.$$

By the quadratic formula we have $a_1^2 = 3$ or 5 so that $a_1 = \pm 4$ or ± 5.

If $a_1 = \pm 4$ then we have $a_2^5 = 10 \cdot 4^2 \cdot (4^2 + 4) = -1$. By (1.6), a_2 is a nonsquare in $\mathbb{F}_{11}$. We then have $a_3 = -a_2^2/(\pm 8) = \pm 4a_2^2$. Denoting a_2 by a this gives us the family of candidate polynomials

$$x^6 \pm 4a^2x^3 + ax^2 \pm 4x \text{ (a a nonsquare).}$$

If $a_1 = \pm 5$ then we have $a_2^5 = 10 \cdot 5^2 \cdot (5^2 + 4) = 1$. By (1.6), a_2 is a nonzero square in $\mathbb{F}_{11}$. We then have $a_3 = -a_2^2/(\pm 10) = \pm a_2^2$. Denoting a_2 by a this gives us the family of candidate polynomials

$$x^6 \pm a^2x^3 + ax^2 \pm 5x \text{ (a a nonzero square).}$$

Routine checking shows that all of the polynomials given satisfy the remaining powers in Theorem 1.5, so they are indeed **PP**s. □

3.4 Degree 6 PPs of $\mathbb{F}_{6m+3}$

If $q = p^r = 6m + 3$ then $p = 3$; the goal of this section is to characterise all degree 6 **PP**s over finite fields of the form $\mathbb{F}_{3^r}$. Note that we are only interested in $r \geqslant 2$, because any degree 6 **PP** of $\mathbb{F}_3$ may be reduced mod $x^3 - x$ to a linear polynomial (by Lemma 1.2 and Corollary 1.7). So **PP**s of $\mathbb{F}_3$ cannot be true degree 6 polynomials.

Although normalisation in the sense of Definition 1.3 only allows us to restrict the constant term and the coefficient of x^6, the following lemma uses a linear transformation to additionally remove the coefficient of either x^5 or x^4. It shows that if we can characterise all degree 6 **PP**s with at most one x^5 or x^4 term, then via linear transformations we can obtain the full list of **PP**s.

Lemma 3.10. *Let*

$$f(x) = x^6 + a_5x^5 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x$$

be a normalised **PP** *of degree 6 in* $\mathbb{F}_{3^r}$*. If* $a_5 \neq 0$ *then by a transformation of the form* $f(x+b)+c$ *we can remove the* x^4 *term.*

Proof. Expanding $f(x+b)+c$ in $\mathbb{F}_{3^r}$ we have

$$\begin{aligned} f(x+b)+c = x^6 &+ a_5x^5 + (a_4 + 2a_5b)x^4 + (a_3 + a_4b + a_5b^2 + 2b^3)x^3 \\ &+ (a_2 + a_5b^3)x^2 + (a_1 + 2a_2b + a_4b^3 + 2a_5b^4)x \\ &+ (a_1b + a_2b^2 + a_3b^3 + a_4b^4 + a_5b^5 + b^6 + c). \end{aligned}$$

If $a_5 \neq 0$ then set $b = a_4/a_5$ to remove the x^4 term and set $c = -(a_1b + a_2b^2 + a_3b^3 + a_4b^4 + a_5b^5 + b^6)$ to remove the constant term. □

We split our characterisation of degree 6 **PP**s into two cases; first the special case $q = 3^2$, then the general case $q > 3^2$.

3.4.1 Degree 6 PPs of $\mathbb{F}_{3^2}$

In this section $2^{1/2}$ is a symbol for *either* solution of $x^2 - 2 = 0$ in $\mathbb{F}_{3^2}$.

We first consider the case $a_5 = 0$.

Theorem 3.11. *The complete list of* **PP***s of* $\mathbb{F}_{3^2}$ *of the form*

$$f(x) = x^6 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x$$

is given by

$$\begin{gathered} x^6 + a^2x^4 + a^7bx^3 + a^4x^2 + a(2b+1)x, \\ a \neq 0, b \in \{0, 1, 2^{1/2}, 1 + 2^{1/2}\}. \end{gathered}$$

Proof. Let $f(x)$ be a **PP** of $\mathbb{F}_{3^2}$. Then by Hermite's criterion (Theorem 1.5) the reductions of $f(x)^2, f(x)^4$ and $f(x)^5$ modulo $x^9 - x$ have degree $\leqslant 7$. Performing these expansions (routine calculations omitted) and equating the coefficient of x^8 to zero in each case, we get the necessary conditions

$$\begin{cases} a_2 = a_4^2, & (1) \\ 1 + a_2^4 + a_4^4 = 0, & (2) \\ a_1^2a_2^3 + 2a_1^3a_2a_3 + a_3^2 + 2a_1a_3^3 + 2a_1^4a_4 + & \\ \quad 2a_2a_4 + 2a_2^3a_4 + 2a_3^4a_4 + a_4^3 + a_2^2a_4^3 + 2a_1a_3a_4^3 = 0. & (3) \end{cases}$$

From (1) and (2) we have $1 + a_4^4 + a_4^8 = 0$. In particular this shows that $a_4 \neq 0$, so we may let $a_4^8 = 1$ and reduce the equation to $a_4^4 = 1$. By (1.6), a_4 is a nonzero square in $\mathbb{F}_{3^2}$.

Substituting (1) into (3) we have

$$\begin{aligned} 0 &= a_3^2 + 2a_1a_3^3 + 2a_1^4a_4 + 2a_3^4a_4 + 2a_1^3a_3a_4^2 + 2a_1a_3a_4^3 + a_1^2a_4^6 \\ &= (a_1^2a_4^6 + 2a_1a_3a_4^3 + a_3^2) + 2(a_1 + a_3a_4)(a_1^3a_4 + a_3^3). \end{aligned}$$

Multiplying by $a_4^3 \neq 0$ and simplifying via $a_4^4 = 1$ we have

$$\begin{aligned} 0 &= a_4(a_1^2 + 2a_1a_3a_4 + a_3^2a_4^2) + 2(a_1 + a_3a_4)(a_1^3 + a_3^3a_4^3) \\ &= a_4(a_1 + a_3a_4)^2 + 2(a_1 + a_3a_4)^4 \\ &= (a_1 + a_3a_4)^2(a_4 + 2(a_1 + a_3a_4)^2). \end{aligned}$$

Hence either $a_1 = 2a_3a_4$ or $a_4 = (a_1 + a_3a_4)^2$. But if $a_1 = 2a_3a_4$ then the polynomial

$$x^6 + a_4x^4 + a_3x^3 + a_4^2x^2 + 2a_3a_4x$$

has roots at 0 and $a_4^{1/2} \neq 0$, thus failing to be injective. So we must have $a_1 = 2a_3a_4 \pm a_4^{1/2}$.

Thus (1)-(3) are satisfied precisely when:

$$\begin{cases} a_4 \text{ is a nonzero square}, \\ a_2 = a_4^2, \\ a_1 = 2a_3a_4 \pm a_4^{1/2}. \end{cases}$$

It is convenient to give the following parametrisation, where a is an arbitrary nonzero element of $\mathbb{F}_{3^2}$:

$$\begin{cases} a_4 = a^2, \\ a_2 = a^4, \\ a_1 = 2a_3a^2 + a. \end{cases}$$

We have chosen the values a_1, a_2, a_4 to satisfy the powers $2, 4, 5$ in Hermite's criterion. Indeed, it happens that these choices also ensure that the power 7 is satisfied. Hence

$f(x)$ is a **PP** if and only if the reduction of $f(x)^8$ modulo $x^9 - x$ is monic of degree 8. Now we have shown that $f(x)$ must be of the form (with $a \neq 0$)

$$f(x) = x^6 + a^2x^4 + a_3x^3 + a^4x^2 + a(2aa_3 + 1)x.$$

Expanding $f(x)^8$ mod $(x^9 - x)$ and equating the coefficient of x^8 to 1, we have

$$1 + aa_3 + a^2a_3^2 + a^3a_3^3 + 2a^4a_3^4 + a^6a_3^6 = 1.$$

After factorisation this condition becomes

$$aa_3(aa_3 + 2)(a^2a_3^2 - 2)((aa_3 + 2)^2 - 2) = 0,$$

which is satisfied whenever $aa_3 = 0, 1, 2^{1/2}$ or $1 + 2^{1/2}$. Equivalently, $a_3 = 0$, a^{-1}, $2^{1/2}a^{-1}$ or $(1 + 2^{1/2})a^{-1}$. Using $a^{-1} = a^7$ and simplifying gives us the following family of **PP**s:

$$\begin{gathered} x^6 + a^2x^4 + a^7bx^3 + a^4x^2 + a(2b + 1)x, \\ a \neq 0, b \in \{0, 1, 2^{1/2}, 1 + 2^{1/2}\}. \end{gathered}$$

□

We compare this result to other characterisations of this case in the literature. The family of **PP**s given above is equivalent to the original family proposed by Dickson in [6], however we suggest that our parametrisation is much cleaner than his family given by

$$\begin{gathered} x^6 + ax^4 + bx^3 + a^2x^2 + (2ab \pm a^{5/2})x \\ a\ \textit{square}, a \neq 0; b = 0, \pm 2^{1/2}a^{3/2}, \pm a^{3/2},\ \text{or}\ \pm(2^{1/2} + 1)a^{3/2}. \\ \textit{The signs of}\ b\ \textit{to correspond to that of}\ \pm a^{5/2}. \end{gathered}$$

On the other hand, the characterisation given in [8, Theorem 3.14] is incorrect, for, in particular, it suggests that the coefficient of x^4 must be a fourth power.

We now consider the case $a_5 \neq 0$. In light of Lemma 3.10 we may assume that $a_4 = 0$.

Theorem 3.12. *The complete list of* **PP***s of* $\mathbb{F}_{3^2}$ *of the form*

$$f(x) = x^6 + a_5x^5 + a_3x^3 + a_2x^2 + a_1x$$

with $a_5 \neq 0$ *is given by*

$$\begin{gathered} x^6 + ax^5 + a^3x^3 + 2a^4x^2 + 2a^5x \quad (a \neq 0), \\ x^6 + ax^5 + \varphi a^3x^3 + 2\varphi a^4x^2 + 2^{1/2}a^5x \quad (a \neq 0, \varphi = \pm(1 - 2^{1/2})), \\ x^6 + ax^5 + 2a^3x^3 + a^4x^2 + (2 + 2^{1/2})a^5x \quad (a \neq 0). \end{gathered}$$

Proof. If $f(x)$ is a **PP** of $\mathbb{F}_{3^2}$ then by Theorem 1.5 the reductions of $f(x)^2$, $f(x)^4$ and $f(x)^5$ modulo $x^9 - x$ have degree $\leqslant 7$. Performing these expansions and equating the coefficient of x^8 to zero in each case we have

$$\begin{cases} a_2 = 2a_3a_5, & (1)\\ 1 + a_2^4 + a_1^3a_5 + a_1a_5^3 = 0, & (2)\\ a_1^2a_2^3 + 2a_1^3a_2a_3 + a_3^2 + 2a_1a_3^3 + 2a_1a_5 + 2a_2a_3^3a_5 + a_2^3a_5^2 + 2a_3a_5^3 = 0. & (3)\end{cases}$$

First we show that $a_1 \neq 0$ and $a_2 \neq 0$. If $a_2 = 0$ then $a_3 = 0$ by (1), from which it follows from (3) that $a_1 = 0$, in contradiction to (2). If $a_1 = 0$ then substituting (1) into (3) we have

$$a_3^2 + a_3^4a_5^2 + 2a_3a_5^3 + 2a_3^3a_5^5 = 0.$$

Multiplying by $a_5^6 \neq 0$ and simplifying via $a_5^8 = 1$ we have

$$a_3^4 + 2a_3a_5 + 2a_3^3a_5^3 + a_3^2a_5^6 = a_3(a_3 + 2a_5^3)(a_3^2 + a_5^6) = 0.$$

But each of $a_3 = 0$, $a_3 = a_5^3$ and $a_3 = 2^{1/2}a_5^3$ lead to a contradiction in (2). So we must have $a_1 \neq 0$ and $a_2 \neq 0$.

Squaring (2) we have

$$\begin{aligned} 0 &= 1 + 2a_2^4 + a_2^8 + 2a_1^3a_5 + 2a_1a_5^3 + 2a_1^3a_2^4a_5 + 2a_1a_2^4a_5^3 + a_1^6a_5^2 + \\ &\quad 2a_1^4a_5^4 + a_1^2a_5^6 \\ &= 2 + 2a_2^4 + a_2^8 + 2(a_1^3a_5 + a_1a_5^3 + 1) + a_2^4(2a_1^3a_5 + 2a_1a_5^3) + a_1^6a_5^2 + \\ &\quad 2a_1^4a_5^4 + a_1^2a_5^6 \\ &= 2 + 2a_2^4 + a_2^8 + a_2^4 + a_2^4(1 + a_2^4) + a_1^6a_5^2 + 2a_1^4a_5^4 + a_1^2a_5^6 \\ &= 2 + a_2^4 + 2a_2^8 + a_1^6a_5^2 + 2a_1^4a_5^4 + a_1^2a_5^6. \end{aligned}$$

But $a_2^8 = 1$ since $a_2 \neq 0$, so we have

$$\begin{aligned} 0 &= (1 + a_2^4) + a_1^6a_5^2 + 2a_1^4a_5^4 + a_1^2a_5^6 \\ &= 2a_1^3a_5 + 2a_1a_5^3 + a_1^6a_5^2 + 2a_1^4a_5^4 + a_1^2a_5^6. \end{aligned}$$

Dividing by $a_1a_5 \neq 0$ and writing $a_1 = \eta a_5^5$ we have

$$\begin{aligned} 0 &= 2a_1^2 + a_1^5a_5 + 2a_5^2 + 2a_1^3a_5^3 + a_1a_5^5 \\ &= 2 + a_5^8\eta + 2a_5^8\eta^2 + 2a_5^{16}\eta^3 + a_5^{24}\eta^5 \\ &= \eta^5 + 2\eta^3 + 2\eta^2 + \eta + 2 \\ &= (\eta + 1)(\eta^2 + 1)((\eta + 1)^2 + 1). \end{aligned}$$

Hence $\eta = 2, 2^{1/2}$ or $2 + 2^{1/2}$.

If $\eta = 2$ then $a_1 = 2a_5^5$, and (1)-(3) reduce to

$$\begin{cases} a_2 = 2a_3a_5, & (1) \\ a_2^4 = 1, & (2) \\ a_3^4a_5^2 + 2a_3a_5^3 + 2a_3^3a_5^5 + a_5^6 = a_5^2(a_3 - a_5^3)^4 = 0. & (3) \end{cases}$$

(1)-(3) are satisfied precisely when $a_3 = a_5^3$ and $a_2 = 2a_5^4$. Then one may check that for any $a_5 \neq 0$ the powers 7 and 8 in Hermite's criterion are also satisfied, so we have the following family of **PP**s

$$x^6 + ax^5 + a^3x^3 + 2a^4x^2 + 2a^5x \quad (a \neq 0).$$

Now suppose that $\eta = 2^{1/2}$. Note that although $2^{1/2}$ may refer to *either* square root of 2 in $\mathbb{F}_{3^2}$ we assume that the particular choice is fixed. Then $a_1 = 2^{1/2}a_5^5$, and (1)-(3) reduce to

$$\begin{cases} a_2 = 2a_3a_5, & (1) \\ a_2^4 = 2, & (2) \\ (1 - 2^{1/2})a_3^2 + a_3^4a_5^2 + 2a_3a_5^3 - 2^{1/2}a_3^3a_5^5 - 2^{1/2}a_5^6 = 0. & (3) \end{cases}$$

Multiplying (3) by a_5^2 and letting $a_3^4a_5^4 = a_2^4 = 2$ and $a_3 = \varphi a_5^3$ we have

$$-2^{1/2}\varphi^3 + (1 - 2^{1/2})\varphi^2 + 2\varphi - (1 + 2^{1/2}) = 0.$$

The roots of this polynomial are $\varphi = -1 + 2^{1/2}, 1 - 2^{1/2}, -1 - 2^{1/2}$. Letting $a_5 = a$ we have reduced to the following candidates

$$x^6 + ax^5 + \varphi a^3x^3 + 2\varphi a^4x^2 + 2^{1/2}a^5x,$$
$$a \neq 0, \varphi \in \{\pm(1 - 2^{1/2}), -1 - 2^{1/2}\}.$$

If $\varphi = -1 - 2^{1/2}$ then this polynomial has roots 0 and $-2^{1/2}a \neq 0$, thus failing to be injective. However if $\varphi = \pm(1 - 2^{1/2})$ then one may verify that (1)-(3) as well as the powers 7 and 8 in Hermite's criterion are satisfied. This gives us the family

$$x^6 + ax^5 + \varphi a^3x^3 + 2\varphi a^4x^2 + 2^{1/2}a^5x,$$
$$a \neq 0, \varphi = \pm(1 - 2^{1/2}).$$

Finally, if $\eta = 2 + 2^{1/2}$ then $a_1 = (2 + 2^{1/2})a_5^5$, and (1)-(3) reduce to

$$\begin{cases} a_2 = 2a_3a_5, & (1) \\ a_2^4 = 1, & (2) \\ 0 = (1 - 2^{1/2})a_5^6 + 2^{1/2}a_3^3a_5^5 + 2a_3a_5^3 + a_3^4a_5^2 - 2^{1/2}a_3^2. & (3) \end{cases}$$

Multiplying (3) by a_5^2 and letting $a_3^4 a_5^4 = a_2^4 = 1$ and $a_3 = \varphi a_5^3$ we have

$$2^{1/2}\varphi^3 - 2^{1/2}\varphi^2 - \varphi - (1 + 2^{1/2}) = 0.$$

The only root is $\varphi = 2$, and the resulting family satisfies (1)-(3) as well as the powers 7 and 8 in Hermite's criterion:

$$x^6 + ax^5 + 2a^3x^3 + a^4x^2 + (2 + 2^{1/2})a^5x \quad (a \neq 0).$$

□

3.4.2 Degree 6 PPs of $\mathbb{F}_{3^r}$, $r > 2$

We now address the more general case of classifying degree 6 **PP**s of $\mathbb{F}_{3^r}$ for all $r > 2$. We will require the 3-adic expansion of $m = (3^{r-1} - 1)/2$:

$$m = 1 + 3 + \cdots + 3^{r-3} + 3^{r-2}. \tag{3.7}$$

Lemma 3.13. *Let $q = 3^r = 6m + 3$ where $r > 2$. Then $1 < m < q - 8$ and $m \equiv 1$ mod 3.*

Proof. We have $m = (q-3)/6 < q - 8$ if and only if $q > 9$, which is true since $r > 2$. Similarly, $(q-3)/6 > 1$ if and only if $q > 9$. It is immediate from (3.7) that $m \equiv 1$ mod 3. □

As with the case $q = 6m + 5$ we use Hermite's criterion to derive necessary equations in the coefficients of a normalised **PP** $f(x)$. Again we observe that $f(x)^{m+1}$ is the first power of f with degree exceeding $q - 1$. Hence $m + 1$ is the first useful power to apply in Hermite's criterion.

In the next theorem we reduce the characterisation problem to the case $a_5 \neq 0$, but we will need a lemma first. Using the powers $m + 1, m + 4$ and $3m + 1$ in Hermite's criterion we determine a set of necessary equations in the coefficients of a degree 6 **PP** satisfying $a_5 = 0$. The reward for this long and tricky lemma is that the equations will be proven inconsistent in $\mathbb{F}_{3^r}$, thus showing that the case $a_5 = 0$ is empty.

Lemma 3.14. *Suppose that*

$$f(x) = x^6 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x \in \mathbb{F}_q[x]$$

is a **PP** *of $\mathbb{F}_q$, where $q = 3^r = 6m + 3$. If $r > 2$ then we have*

$$\begin{cases} a_2 = a_4^2, & (1)\\ 2a_1^2a_2^3 + a_1^3a_2a_3 + 2a_2a_3^6 + a_1^4a_4 + & \\ \quad a_3^6a_4^2 + a_2a_3^4a_4^3 + a_1a_3^3a_4^4 + 2a_2^3a_4^5 + a_1^2a_4^6 = 0, & (2)\\ 1 + a_4^{3m+1} + a_2^{3m+1} = 0. & (3) \end{cases}$$

Proof. Suppose that $f(x)$ is a **PP** of $\mathbb{F}_q$, where $q = 3^r$ and $r > 2$. By Lemma 3.13 we have that $m+1$ and $m+4$ are nonzero mod 3, and

$$2 < m+1, m+4 < q-4.$$

We also have $3m+1 \equiv 1 \not\equiv 0$ mod 3 and that

$$1 \leqslant 3m+1 \leqslant 6m+1 = q-2 \text{ for all } m \geqslant 0.$$

So by Theorem 1.5 the reductions of $f(x)^{m+1}, f(x)^{m+4}$ and $f(x)^{3m+1}$ modulo $x^q - x$ each have degree $\leqslant q-2$.

We use the multinomial theorem to expand these powers. By Theorem 3.1 we have, for any positive integer t,

$$f(x)^t = \sum_{\substack{k_1+k_2+k_3\\+k_4+k_6=t}} \binom{t}{k_1, k_2, k_3, k_4, k_6} a_1^{k_1} a_2^{k_2} a_3^{k_3} a_4^{k_4} \cdot x^{k_1+2k_2+3k_3+4k_4+6k_6}. \tag{3.8}$$

First consider the expansions of $f(x)^{m+1}$ and $f(x)^{m+4}$. We are interested in the terms $x^{i(q-1)}$, but since $2(q-1) > 6(m+1) = q+3$ for all $q > 5$ and $2(q-1) > 6(m+4) = q+21$ for all $q > 23$ there are no terms of the form $x^{i(q-1)}, i \geqslant 2$. Hence, in each case, we only need to find the coefficient of $x^{q-1} = x^{6m+2}$. For the power $f(x)^{m+1}$ this amounts to solving the system

$$\begin{cases} k_1 + k_2 + k_3 + k_4 + k_6 = m+1, & (a) \\ k_1 + 2k_2 + 3k_3 + 4k_4 + 6k_6 = 6m+2, & (b) \end{cases}$$

for which the solutions are

$$\begin{array}{c|c|c|c|c} k_1 & k_2 & k_3 & k_4 & k_6 \\ \hline 0 & 1 & 0 & 0 & m \\ 0 & 0 & 0 & 2 & m-1 \end{array} . \tag{3.9}$$

Similarly, to find the coefficient of x^{6m+2} in $f(x)^{m+4}$ we must solve the system

$$\begin{cases} k_1 + k_2 + k_3 + k_4 + k_6 = m+4, & (a) \\ k_1 + 2k_2 + 3k_3 + 4k_4 + 6k_6 = 6m+2. & (b) \end{cases}$$

There are in fact 34 solutions. A partial list is

$$\begin{array}{c|c|c|c|c}
k_1 & k_2 & k_3 & k_4 & k_6 \\
\hline
4 & 0 & 0 & 1 & m-1 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
3 & 0 & 1 & 2 & m-2 \\
2 & 2 & 0 & 2 & m-2 \\
2 & 1 & 2 & 1 & m-2 \\
\vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 4 & 5 & m-5 \\
0 & 0 & 2 & 8 & m-6 \\
0 & 0 & 0 & 11 & m-7
\end{array}. \tag{3.10}$$

Now (3.9) and (3.10) determine terms in $f(x)^{m+1}$ and $f(x)^{m+4}$, respectively, of the form

$$\binom{m+1}{k_1, k_2, k_3, k_4, k_6} a_1^{k_1} a_2^{k_2} a_3^{k_3} a_4^{k_4} x^{q-1} \text{ and } \binom{m+4}{k_1, k_2, k_3, k_4, k_6} a_1^{k_1} a_2^{k_2} a_3^{k_3} a_4^{k_4} x^{q-1}.$$

For each solution in (3.9) and (3.10) we apply Theorem 3.2 to calculate the corresponding multinomial coefficient mod 3. We give two examples of this below.

Consider the first solution in (3.10). Using the 3-adic expansion of m from (3.7) we have

$$\begin{aligned}
m+4 &= 2 + 2 \cdot 3 + 1 \cdot 3^2 + \cdots + 1 \cdot 3^{r-3} + 1 \cdot 3^{r-2} \\
m-1 &= 0 + 1 \cdot 3 + 1 \cdot 3^2 + \cdots + 1 \cdot 3^{r-3} + 1 \cdot 3^{r-2} \\
4 &= 1 + 1 \cdot 3 + 0 \cdot 3^2 + \cdots + 0 \cdot 3^{r-3} + 0 \cdot 3^{r-2} \\
1 &= 1 + 0 \cdot 3 + 0 \cdot 3^2 + \cdots + 0 \cdot 3^{r-3} + 0 \cdot 3^{r-2}
\end{aligned}$$

We observe that there are no 'carries' in the sum $(m+4) = (m-1) + 4 + 1$, so by Theorem 3.2 the multinomial coefficient $\binom{m+4}{4,0,0,1,m-1}$ is nonzero mod 3, and we have

$$\begin{aligned}
\binom{m+4}{4,0,0,1,m-1} &\equiv \binom{2}{1,0,0,1,0} \binom{2}{1,0,0,1,1} \binom{1}{0,0,0,0,1} \cdots \\
&\qquad \binom{1}{0,0,0,0,1} \text{ mod } 3 \\
&\equiv 2 \cdot 2 \text{ mod } 3 \\
&\equiv 1 \text{ mod } 3.
\end{aligned}$$

Thus we get a term of the form $a_1^4 a_4 x^{q-1}$ in the expansion of $f(x)^{m+4} \bmod (x^q - x)$.

On the other hand, for the second solution listed in (3.10) we have

$$\begin{aligned}
m+4 &= 2 + 2\cdot 3 + 1\cdot 3^2 + \cdots + 1\cdot 3^{r-3} + 1\cdot 3^{r-2}\\
m-2 &= 2 + 0\cdot 3 + 1\cdot 3^2 + \cdots + 1\cdot 3^{r-3} + 1\cdot 3^{r-2}\\
3 &= 0 + 1\cdot 3 + 0\cdot 3^2 + \cdots + 0\cdot 3^{r-3} + 0\cdot 3^{r-2}\\
1 &= 1 + 0\cdot 3 + 0\cdot 3^2 + \cdots + 0\cdot 3^{r-3} + 0\cdot 3^{r-2}\\
2 &= 2 + 0\cdot 3 + 0\cdot 3^2 + \cdots + 0\cdot 3^{r-3} + 0\cdot 3^{r-2}
\end{aligned}$$

In this case there *is* a carry in the sum $(m+4) = (m-2) + 3 + 1 + 2$, so by Theorem 3.2 the multinomial coefficient $\binom{m+4}{3,0,1,2,m-2}$ is zero mod 3.

By similar computations (this process can be automated) we calculate the remaining binomial coefficients mod 3, and hence the coefficients of x^{q-1} in $f(x)^{m+1}$ and $f(x)^{m+4}$ mod $x^q - x$. Equating them to zero we have, respectively,

$$\begin{cases}
2a_2 + a_4^2 = 0, & (1)\\
2a_1^2a_2^3 + a_1^3a_2a_3 + 2a_2a_3^6 + a_1^4a_4 + a_3^6a_4^2 + & \\
\quad a_2^4a_4^3 + a_2a_3^4a_4^3 + a_1a_3^3a_4^4 + 2a_2^3a_4^5 + a_1^2a_4^6 + 2a_4^9a_2 + a_4^{11} = 0. & (2)
\end{cases}$$

Note that the last two terms in (2) do not appear in the case $r = 3$. When $r > 3$ these terms become, by (1),

$$2a_4^9a_2 + a_4^{11} = 3a_4^{11} = 0.$$

Hence we can omit the last two terms in (2) in all cases.

Now consider the power $f(x)^{3m+1}$. We are interested in terms of the form $x^{i(q-1)} = x^{i(6m+2)}$. Now $\deg\left(f(x)^{3m+1}\right) = 6(3m+1) = 3(6m+2)$, so we are interested in the coefficients of x^{6m+2}, $x^{2(6m+2)}$, $x^{3(6m+2)}$. By (3.8) this amounts to solving, for each $i \in \{1,2,3\}$, the system

$$\begin{cases}
k_1 + k_2 + k_3 + k_4 + k_6 = 3m+1, & (a)\\
k_1 + 2k_2 + 3k_3 + 4k_4 + 6k_6 = 2i(3m+1). & (b)
\end{cases} \tag{3.11}$$

For $i = 3$ it is immediate that the only solution is

k_1	k_2	k_3	k_4	k_6
0	0	0	0	$3m+1$

For $i = 2$ there are many solutions, but we only solve for those for which the multinomial coefficient $\binom{3m+1}{k_1,k_2,k_3,k_4,k_6}$ is nonzero mod 3. To apply Theorem 3.2 we need expressions for the 3-adic expansions of $3m+1, k_1, k_2, k_3, k_4, k_6$. Now by (3.7) we have

$$3m+1 = 1 + 1\cdot 3 + \cdots + 1\cdot 3^{r-2} + 1\cdot 3^{r-1},$$

and we will denote 3-adic expansions of k_1, k_2, k_3, k_4, k_6 by

$$\begin{aligned} k_1 &= b_{10} + b_{11} \cdot 3 + \cdots + b_{1(r-2)} \cdot 3^{r-2} + b_{1(r-1)} \cdot 3^{r-1} \\ &\vdots \\ k_6 &= b_{60} + b_{61} \cdot 3 + \cdots + b_{6(r-2)} \cdot 3^{r-2} + b_{6(r-1)} \cdot 3^{r-1} \end{aligned}$$

Then by Theorem 3.2 the multinomial coefficient $\binom{3m+1}{k_1,k_2,k_3,k_4,k_6}$ is nonzero mod 3 if and only if

$$b_{1j} + b_{2j} + b_{3j} + b_{4j} + b_{6j} = 1 \text{ for all } 0 \leqslant j \leqslant r-1. \tag{3.12}$$

Then (3.12) implies $(3.11, a)$. Rewriting $(3.11, b)$ with the 3-adic expansions we have

$$\begin{aligned} (b_{10} + 2b_{20} + 3b_{30} + 4b_{40} + 6b_{60}) + (b_{11} + 2b_{21} + 3b_{31} + 4b_{41} + 6b_{61}) \cdot 3 + \cdots + \\ (b_{1(r-1)} + 2b_{2(r-1)} + 3b_{3(r-1)} + 4b_{4(r-1)} + 6b_{6(r-1)})3^{r-1} \\ = 1 + 2 \cdot 3 + \cdots + 2 \cdot 3^{r-1} + 3^r \end{aligned} \tag{3.13}$$

By (3.12) and (3.13) we must have $b_{2j} = 0$ for all j. For clearly $b_{20} \neq 1$, and if $b_{2j} = 1$ for some $1 \leqslant j \leqslant r-2$ then it follows that $b_{2(j+1)} = 1$. We must then conclude that $b_{2j} = b_{2(j+1)} = \cdots = b_{2(r-1)} = 1$, but then the *LHS* of (3.13) is too small. So we must have $b_{2j} = 0$ for all j. By a similar argument we have $b_{1j} = 0$ for all j, because if $b_{1j} = 1$ for some $0 \leqslant j \leqslant r-2$ then we must have $b_{2(j+1)} = 1$. Hence (3.13) reduces to

$$\begin{aligned} (3b_{30} + 4b_{40} + 6b_{60}) + (3b_{31} + 4b_{41} + 6b_{61}) \cdot 3 + \cdots + \\ (3b_{3(r-1)} + 4b_{4(r-1)} + 6b_{6(r-1)}) \cdot 3^{r-1} \\ = 1 + 2 \cdot 3 + \cdots + 2 \cdot 3^{r-1} + 3^r \end{aligned} \tag{3.14}$$

It is clear that the only possible solution satisfying (3.12) and (3.14) is $b_{40} = b_{41} = \cdots = b_{4(r-1)} = 1$ with all other terms zero. Hence $k_4 = 1 + 3 + \cdots + 3^{r-1} = 3m+1$ and the solution is given by

k_1	k_2	k_3	k_4	k_6
0	0	0	$3m+1$	0

For $i = 1$ a similar (but easier) argument shows that the only solution with nonzero multinomial coefficient is $k_2 = 1 + 3 + \cdots + 3^{r-1} = 3m+1$ and the solution is given by

k_1	k_2	k_3	k_4	k_6
0	$3m+1$	0	0	0

Hence the term in x^{q-1} in the reduction of $f(x)^{3m+1}$ mod $(x^q - x)$ is given by

$$\left(\binom{3m+1}{0,0,0,0,3m+1} + \binom{3m+1}{0,0,0,3m+1,0} a_4^{3m+1} + \binom{3m+1}{0,3m+1,0,0,0} a_2^{3m+1}\right) x^{q-1}.$$

Thus Theorem 1.5 requires that

$$1 + a_4^{3m+1} + a_2^{3m+1} = 0. \quad (3)$$

□

The following theorem rewards the lengthy and tricky calculations in the previous lemma by reducing the characterisation problem to the case $a_5 \neq 0$.

Theorem 3.15. *If $r > 2$ then there are no* **PP***s of $\mathbb{F}_{3^r}$ of the form*

$$f(x) = x^6 + a_4x^4 + a_3x^3 + a_2x^2 + a_1x.$$

Proof. If $f(x)$ is a **PP** of $\mathbb{F}_{3^r}$ then by Lemma 3.14 we have

$$\begin{cases} a_2 = a_4^2, & (1) \\ 2a_1^2a_2^3 + a_1^3a_2a_3 + 2a_2a_3^6 + a_1^4a_4 + & \\ \quad a_3^6a_4^2 + a_2^4a_4^3 + a_2a_3^4a_4^3 + a_1a_3^3a_4^4 + 2a_2^3a_4^5 + a_1^2a_4^6 = 0, & (2) \\ 1 + a_4^{3m+1} + a_2^{3m+1} = 0. & (3) \end{cases}$$

Substituting (1) into (3) we have

$$1 + a_4^{3m+1} + a_4^{6m+2} = 0. \tag{3.15}$$

This shows that $a_4 \neq 0$, so we have $a_4^{6m+2} = a_4^{q-1} = 1$. We may therefore write (3.15) as

$$a_4^{3m+1} = a_4^{(q-1)/2} = 1.$$

By (1.6), a_4 is a nonzero square in $\mathbb{F}_{3^r}$.

Substituting (1) into (2) we have

$$\begin{aligned} 0 &= a_1^4a_4 + a_1^3a_3a_4^2 + a_1a_3^3a_4^4 + a_3^4a_4^5 \\ &= a_4(a_1^4 + a_1^3a_3a_4 + a_1a_3^3a_4^3 + a_3^4a_4^4) \\ &= a_4(a_1 + a_3a_4)^4. \end{aligned}$$

Since $a_4 \neq 0$ we have $a_1 = 2a_3a_4$. But the polynomial

$$x^6 + a_4x^4 + a_3x^3 + a_4^2x^2 + 2a_3a_4x$$

has roots at 0 and $a_4^{1/2} \neq 0$, thus failing to be injective. □

Since we know that $a_5 \neq 0$ we will therefore let $a_4 = 0$ by Lemma 3.10. We first give a full characterisation for the case $r = 3$.

Theorem 3.16. *The complete list of* **PP***s of* $\mathbb{F}_{3^3}$ *of the form*

$$f(x) = x^6 + a_5x^5 + a_3x^3 + a_2x^2 + a_1x$$

with $a_5 \neq 0$ *is given by*

$$x^6 + ax^5 + 2a^4x^2 \quad (a \neq 0).$$

Proof. If $f(x)$ is a **PP** of $\mathbb{F}_{3^3}$, then by Theorem 1.5 the reductions of $f(x)^5$, $f(x)^7$, $f(x)^8$ and $f(x)^{13}$ modulo $x^{27} - x$ must have degree $\leqslant 25$. These require, respectively,

$$\begin{cases} a_5^4 + a_3a_5 + a_2 = 0, & (1) \\ a_2^3a_5^4 + a_2a_3^3a_5^3 + a_1^3a_5 + a_2^4 = 0, & (2) \\ 2a_1^2a_2^3 + a_1^3a_2a_3 + 2a_2a_3^6 + a_2^3a_3^3a_5 + & \\ \quad 2a_3^7a_5 + a_1^3a_2a_5^3 + a_2^4a_3a_5^3 + 2a_1^2a_3^3a_5^3 + a_1^3a_3a_5^4 = 0, & (3) \\ 1 + a_2^{13} + a_1^3a_2^9a_5 + a_1^9a_2a_5^3 + a_1a_2^3a_5^9 = 0. & (4) \end{cases}$$

Applying (1) to (2) we have

$$\begin{aligned} 0 &= a_5(2a_1^3 + a_3^3a_5^6 + 2a_3a_5^{12} \\ &= a_5(2a_1 + a_3a_5^2 + 2a_3^9a_5^4)^3. \end{aligned}$$

Hence

$$a_1 = a_3a_5^2 + 2a_3^9a_5^4. \tag{3.16}$$

If $a_3 = 0$ then by (3.16) we have $a_1 = 0$. By checking the remaining powers in Hermite's criterion, the resulting family

$$x^6 + ax^5 + 2a^4x^2 \quad (a \neq 0)$$

are shown to be **PP**s.

Now suppose that $a_3 \neq 0$. Applying (1) and (3.16) to (3) we have

$$\begin{aligned} 0 &= 2a_3^3a_5^{13} + a_3^{10}a_5^{18} + 2a_3a_5^{19} + a_3^{18}a_5^{20} \\ &= a_3a_5^{13}(2a_3^2 + a_3^9a_5^5 + 2a_5^6 + a_3^{17}a_5^7). \end{aligned}$$

Dividing by $a_3a_5^{13} \neq 0$ and letting $a_3 = \eta a_5^3$, this becomes

$$\eta^{17} + \eta^9 + 2\eta^2 + 2.$$

Multiplying this equation by η^9 and letting $\eta^{26} = 1$ and $\eta^{11} = \eta^{52} \cdot \eta^{11} = \eta^{63}$, we have

$$\begin{aligned} 0 &= \eta^{63} + 2\eta^{18} + \eta^9 + 2 \\ &= (\eta + 2)^{18}(\eta^2 + 1)^9(\eta^3 + 2\eta^2 + 2\eta + 2)^9 \end{aligned}$$

Now the root $\eta = 1$ can be ignored since the polynomial

$$x^6 + a_5x^5 + a_5^3x^3 + a_5^4x^2$$

has roots at 0 and $-a_5 \neq 0$, and $\eta^2 = -1$ is impossible since $\mathbb{F}_{3^3}$ is a degree 3 extension of $\mathbb{F}_3$. So we must have

$$\eta^3 = \eta^2 + \eta + 1.$$

Substituting $a_1 = a_5^5(\eta + 2\eta^9), a_2 = 2a_5^4(1+\eta)$ and $a_3 = a_5^3\eta$ into (4) and simplifying gives

$$2\eta(\eta^3 + 2\eta + 2)(\eta^3 + \eta^2 + 2)(\eta^3 + \eta^2 + 2\eta + 1)(\eta^3 + 2\eta^2 + 1) = 0.$$

But using $\eta^3 = \eta^2 + \eta + 1$ this simplifies to

$$2\eta^4(\eta + 2)^2(\eta^2 + 1) = 0,$$

in contradiction to $\eta \notin \{0, 1\}$ and $\eta^2 \neq -1$. □

Finally, we show that there are no **PP**s of $\mathbb{F}_{3^r}$ when $r > 3$.

Theorem 3.17. *If $r > 3$ and $a_5 \neq 0$ then there are no* **PP***s of $\mathbb{F}_{3^r}$ of the form*

$$f(x) = x^6 + a_5x^5 + a_3x^3 + a_2x^2 + a_1x.$$

Proof. Suppose $f(x)$ is a **PP** of $\mathbb{F}_{3^r}$ and $r > 3$. By Lemma 3.13 we have $1 \leqslant m \leqslant q-8$ and $m \equiv 1 \bmod 3$, so by Theorem 1.5 the reductions of $f(x)^{m+1}$ and $f(x)^{m+3}$ modulo $x^q - x$ have degree $\leqslant q - 2$. By similar calculations to Lemma 3.14 we determine that these conditions require

$$\begin{cases} a_2 = 2a_3a_5 + 2a_5^4, & (1) \\ a_2^4 + a_1^3a_5 + a_2a_3^3a_5^3 + a_2^3a_5^4 + a_2a_5^{12} + 2a_5^{16} = 0. & (2) \end{cases}$$

Substituting (1) into (2) we have

$$\begin{aligned} 0 &= 2a_1^3a_5 + a_3^3a_5^7 + 2a_5^{16} \\ &= 2a_5(a_1 + 2a_3a_5^2 + a_5^5)^3. \end{aligned}$$

Since $a_5 \neq 0$ we must have $a_1 = a_3a_5^2 + 2a_5^5$. But the polynomial

$$x^6 + a_5x^5 + a_3x^3 + (2a_3a_5 + 2a_5^4)x^2 + (a_3a_5^2 + 2a_5^5)x$$

has roots 0 and $-a_5 \neq 0$, thus failing to be injective, so is not a **PP**. □

3.5 Normalised PPs of Degree 6

In Theorems 3.8 - 3.17 we derived the complete classification of degree 6 **PP**s of $\mathbb{F}_q$ up to transformations of the form

$$cf(x + b) + d, \text{ where } b, c, d \in \mathbb{F}_q, c \neq 0.$$

These are listed in Table 3.1.

(1) $x^6 \pm 2x$, $q = 11$.

(2) $x^6 \pm 4x$, $q = 11$.

(3) $x^6 \pm a^2x^3 + ax^2 \pm 5x$, a a nonzero square, $q = 11$.

(4) $x^6 \pm 4a^2x^3 + ax^2 \pm 4x$, a not square, $q = 11$.

(5) $x^6 + a^2x^4 + a^7bx^3 + a^4x^2 + a(2b+1)x$, $a \neq 0, b \in \{0, 1, 2^{1/2}, 1 + 2^{1/2}\}$, $q = 3^2$.

(6) $x^6 + ax^5 + a^3x^3 + 2a^4x^2 + 2a^5x$, $a \neq 0$, $q = 3^2$.

(7) $x^6 + ax^5 + \varphi a^3x^3 + 2\varphi a^4x^2 + 2^{1/2}a^5x$, $a \neq 0, \varphi = \pm(1 - 2^{1/2})$, $q = 3^2$.

(8) $x^6 + ax^5 + 2a^3x^3 + a^4x^2 + (2 + 2^{1/2})a^5x$, $a \neq 0$, $q = 3^2$.

(9) $x^6 + ax^5 + 2a^4x^2$, $a \neq 0$, $q = 3^3$.

Table 3.1: *Classification of degree 6* **PP***s of* $\mathbb{F}_q$ *(q odd) up to linear transformations.*

We remark that this list agrees with the original list in [6], except that Dickson fails to specify that a is not allowed to be zero in (3) and (6-9). Additionally, the family of **PP**s given in (5) has a cleaner parametrisation than in the original list.

We note, however, that this is *not* the complete list of normalised degree 6 **PP**s in the sense of Definition 1.3, because in the cases $q = 3^2$ and $q = 3^3$ we used a second linear transformation to ensure that the coefficient of x^5 or x^4 was zero. So, for example, the polynomial

$$f(x) = x^6 + x^5 + x^4 + x^2 \in \mathbb{F}_{3^2}[x]$$

is a normalised **PP** of $\mathbb{F}_{3^2}$ not appearing in the above list. Similarly, the following polynomial is a normalised **PP** of $\mathbb{F}_{3^3}$ not in the list:

$$g(x) = x^6 + x^5 + 2x^4 \in \mathbb{F}_{3^3}[x].$$

So, although the above list completely classifies degree 6 **PP**s up to linear transformations, it is incorrect to call it a complete list of *normalised* **PP**s. This is the claim made by Dickson in [6] when he said his list was a *complete list of reduced quantics*. Although the distinction is minor, we suggest this ambiguity has caused confusion and is the reason that Dickson's characterisation has been questioned.

We now convert the list (1-9) into the complete list of normalised **PP**s of degree 6, which we feel is necessary for the sake of consistency and avoiding future confusion. We will then be able to insert the degree 6 classification unambiguously into the complete list of normalised (in the sense of the globally accepted definition) **PP**s of degree up to 6. Recall from Section 3.4 that in the case $p = 3$ and $a_5 \neq 0$ we used a linear transformation to remove the x^4 term (see Lemma 3.10). To recover the list of normalised **PP**s represented by (6-9) we must apply transformations of the form

$$f(x) = g(x+b) + c,$$

where b is arbitrary and c is chosen so that the resulting polynomial $f(x)$ satisfies $f(0) = 0$. Applying these transformations to the polynomials (6-9), and simplifying, we obtain the complete list of normalised **PP**s of degree 6 in Table 3.2. See Appendix A for the complete list of normalised **PP**s of degree $\leqslant 6$.

(1) $x^6 \pm 2x$, $q = 11$.

(2) $x^6 \pm 4x$, $q = 11$.

(3) $x^6 \pm a^2x^3 + ax^2 \pm 5x$, a a nonzero square, $q = 11$.

(4) $x^6 \pm 4a^2x^3 + ax^2 \pm 4x$, a not square, $q = 11$.

(5) $x^6 + a^2x^4 + a^7bx^3 + a^4x^2 + a(2b+1)x$, $a \neq 0, b \in \{0, 1, 2^{1/2}, 1 + 2^{1/2}\}$, $q = 3^2$.

(6) $x^6 + ax^5 + 2abx^4 + (a^3 + ab^2 + 2b^3)x^3 + (2a^4 + ab^3)x^2 + (2a^5 + a^4b + 2ab^4)x$, $a \neq 0$, b arbitrary, $q = 3^2$.

(7) $x^6 + ax^5 + 2abx^4 + (ab^2 + 2b^3 + a^3\varphi)x^3 + (ab^3 + 2a^4\varphi)x^2 + (2^{1/2}a^5 + 2ab^4 + a^4b\varphi)x$, $a \neq 0$, b arbitrary, $\varphi = \pm(1 - 2^{1/2})$, $q = 3^2$.

(8) $x^6 + ax^5 + 2abx^4 + (2a^3 + ab^2 + 2b^3)x^3 + (a^4 + ab^3)x^2 + (2a^5 + 2^{1/2}a^5 + 2a^4b + 2ab^4)x$, $a \neq 0$, b arbitrary, $q = 3^2$.

(9) $x^6 + ax^5 + 2abx^4 + (ab^2 + 2b^3)x^3 + (2a^4 + ab^3)x^2 + (a^4b + 2ab^4)x$, $a \neq 0$, b arbitrary, $q = 3^3$.

Table 3.2: *Complete list of normalised degree 6* **PP***s of* $\mathbb{F}_q$ *(q odd).*

Chapter 4

Orthomorphism Polynomials

4.1 Orthomorphism Polynomials of Finite Fields

We begin by defining orthomorphisms for general finite groups G.

Definition 4.1. Let G be a finite group. Then an *orthomorphism* of G is a permutation Φ of G such that the map $c \mapsto c^{-1}\Phi(c)$ is also a permutation of G.

Orthomorphisms have also been referred to as *orthogonal mappings*. There are numerous reasons to be interested in orthomorphisms, for example for the construction of orthogonal Latin squares.

A closely related concept is that of a *complete mapping* of G, which is a permutation Φ such that the map $c \mapsto c\Phi(c)$ is a permutation of G. Then Φ is an orthomorphism of G if and only if the map $c \mapsto c^{-1}\Phi(c)$ is a complete mapping of G and a complete mapping of G if and only if the map $c \mapsto c\Phi(c)$ is an orthomorphism of G.

In this paper we only consider orthomorphisms of the additive group $\mathbb{F}_q^+$ of a finite field; the interested reader may refer to [8] for orthomorphisms of general groups. Note that by Lemma 1.1 we may assume that an orthomorphism of $\mathbb{F}_q^+$ is a polynomial $f \in \mathbb{F}_q[x]$. We will call such a polynomial an *orthomorphism polynomial.* It is clear that f is an orthomorphism polynomial of $\mathbb{F}_q$ if and only if $f(x)$ and $f(x) - x$ are both **PP**s of $\mathbb{F}_q$.

We begin by stating a fundamental result on the degree of an orthomorphism polynomial of $\mathbb{F}_q$. We already know (by Corollary 1.7) that the reduction modulo $x^q - x$ of a **PP** of $\mathbb{F}_q$ has degree at most $q-2$. In fact for orthomorphism polynomials we have the following stronger bound.

Theorem 4.1. *If $q > 2$ and $f(x)$ is an orthomorphism polynomial of $\mathbb{F}_q$ then the reduction of f modulo $x^q - x$ has degree at most $q - 3$.*

The above theorem was proved by Niederreiter and Robinson [19] for odd q, and by Wan [26] for even q. We refer the reader to [8] for its complete proof.

The following trivial lemma gives us a concept analogous to normalised a permutation polynomials.

Lemma 4.2. *If $f \in \mathbb{F}_q[x]$ is an orthomorphism polynomial of $\mathbb{F}_q$ then so is*

$$g(x) = f(x+b) + d, \text{ where } b, d \in \mathbb{F}_q.$$

By suitable choices of b and d we can ensure that the resulting polynomial $g(x)$ satisfies $g(0) = 0$, and when the degree n of f is not divisible by the characteristic of $\mathbb{F}_q$, the coefficient of x^{n-1} is zero.

Remark 4.1. Unlike with permutation polynomials, it is *not* true that $cf(x)$ is also an orthomorphism polynomial for any $c \neq 0$. For example, $2x$ is always an orthomorphism polynomial of $\mathbb{F}_q$ but x is not.

4.2 Degree 6 Orthomorphism Polynomials

Orthomorphism polynomials of degree up to 5 were classified by Niederreiter and Robinson [19] in 1982. In fact they actually classified complete mapping polynomials, but it is then a simple matter to determine the orthomorphism polynomials since $f(x)$ is a complete mapping polynomial if and only if $f(x) + x$ is an orthomorphism polynomial. In the same paper the authors also resolved the degree 6 case when $\gcd(6, q) = 1$. The reader may find the list of orthomorphism polynomials from these cases in [8]. Using the characterisation of degree 6 **PP**s from Chapter 3 we now proceed to classify all degree 6 orthomorphism polynomials of fields of characteristic 3.

Let $f(x)$ be an orthomorphism polynomial of $\mathbb{F}_{3^r}$, where $r \geqslant 2$. Then by Lemma 4.2 the polynomial $g(x) = f(x+b) + d$ is also an orthomorphism of $\mathbb{F}_{3^r}$. By choosing b and d suitably we can ensure that $g(0) = 0$ and if the coefficient of x^5 is nonzero then the coefficient of x^4 is zero. If we can classify orthomorphisms with these properties then we have a complete classification up to linear transformations. Let $f \in \mathbb{F}_{3^r}[x]$ be a degree 6 polynomial and define the following properties:

(*P1*) $f(0) = 0$.

(*P2*) The coefficient of x^5 is zero.

(*P3*) The coefficient of x^5 is nonzero and the coefficient of x^4 is zero.

Also, recall that in this project the symbol $2^{1/2}$ always represents *either* root of the equation $x^2 + 1 = 0$ in $\mathbb{F}_{3^2}$. It will henceforth be necessary to distinguish between the two solutions, so we let $2^{1/2} \in \{\pm i\}$, where i is a solution fixed throughout.

We first classify the orthomorphism polynomials of $\mathbb{F}_{3^2}$ satisfying (*P1*) and (*P2*).

Theorem 4.3. *The complete list of degree 6 orthomorphism polynomials $f(x)$ of $\mathbb{F}_{3^2}$ satisfying (P1) and (P2) is given by*

$$cx^6 + c^7x^4 + c^5x^2 + 2x \quad (c \neq 0),$$
$$cx^6 + c^7x^4 - 2^{1/2}c^2x^3 + c^5x^2 + (2 + 2^{1/2})x \quad (c \neq 0).$$

Proof. Recall that Table 3.1 (5) is the complete classification of monic **PP**s of $\mathbb{F}_{3^2}$ satisfying (*P1*) and (*P2*). Multiplying this family by an arbitrary constant $c \neq 0$ (to remove the monoticity restriction), we recover the complete list of **PP**s satisfying (*P1*) and (*P2*):

$$\begin{gathered} cx^6 + a^2cx^4 + a^7bcx^3 + a^4cx^2 + ac(2b+1)x, \\ a, c \neq 0, b \in \{0, 1, \pm i, 1 \pm i\}. \end{gathered} \tag{4.1}$$

If $f(x)$ is an orthomorphism polynomial of $\mathbb{F}_{3^2}$ then it is necessarily of the above form; that is,

$$f(x) = cx^6 + a^2cx^4 + a^7bcx^3 + a^4cx^2 + ac(2b+1)x \tag{4.2}$$

for some $a, c \neq 0, b \in \{0, 1, \pm i, 1 \pm i\}$. Hence,

$$f(x) - x = cx^6 + a^2cx^4 + a^7bcx^3 + a^4cx^2 + (ac(2b+1) - 1)x. \tag{4.3}$$

Note that this is again a polynomial satisfying (*P1*) and (*P2*), so f is an orthomorphism polynomial if and only if $f(x) - x$ is of the form (4.1). That is, there must exist $A, C \neq 0, B \in \{0, 1, \pm i, 1 \pm i\}$ such that

$$f(x) - x = Cx^6 + A^2Cx^4 + A^7BCx^3 + A^4Cx^2 + AC(2B+1)x. \tag{4.4}$$

We proceed to equate the coefficients of (4.3) and (4.4). Since clearly it is impossible that $A = a, B = b, C = c$, we have from the coefficients of x^6, x^4, x^3 and x^2 that

$$A = -a, B = -b, C = c.$$

Hence $b \in \{0, \pm i\}$, the largest subset of $\{0, 1, \pm i, 1 \pm i\}$ closed under negation. The coefficient of x then requires

$$ac(2b+1) - 1 = -ac(-2b+1).$$

Rearranging, we find that $a = -c^{-1}$, and substituting this and $b \in \{0, \pm i\}$ into (4.2) and simplifying we have precisely the following orthomorphism polynomials:

$$cx^6 + c^7x^4 - bc^2x^3 + c^5x^2 + (b+2)x \quad (c \neq 0, b \in \{0, \pm i\}).$$

□

Now we consider the case where (*P1*) and (*P3*) are satisfied.

Theorem 4.4. *The complete list of degree 6 orthomorphism polynomials $f(x)$ of $\mathbb{F}_{3^2}$ satisfying (P1) and (P3) is given by*

$$a^5x^6 + 2^{1/2}a^4x^5 + 2^{1/2}a^2x^3 + ax^2 + 2(1+2^{1/2})x \quad (a \neq 0).$$

Proof. From Table 3.1 (6-8) the complete list of **PP**s of $\mathbb{F}_{3^2}$ satisfying (*P1*) and (*P3*) is given by

$$cx^6 + acx^5 + a^3cx^3 + 2a^4cx^2 + 2a^5cx, \quad (a, c \neq 0) \tag{4.5}$$

$$cx^6 + acx^5 + \varphi a^3cx^3 + 2\varphi a^4cx^2 + ia^5cx, \quad (a, c \neq 0, \varphi = \pm(1-i)) \tag{4.6}$$

$$cx^6 + acx^5 + \varphi a^3cx^3 + 2\varphi a^4cx^2 - ia^5cx, \quad (a, c \neq 0, \varphi = \pm(1+i)) \tag{4.7}$$

$$cx^6 + acx^5 + 2a^3cx^3 + a^4cx^2 + (2+i)a^5cx, \quad (a, c \neq 0) \tag{4.8}$$

$$cx^6 + acx^5 + 2a^3cx^3 + a^4cx^2 + (2-i)a^5cx. \quad (a, c \neq 0) \tag{4.9}$$

As before, note that if $f(x)$ is a polynomial satisfying (*P1*) and (*P3*) then $f(x) - x$ also satisfies (*P1*) and (*P3*). Hence, f is an orthomorphism polynomial if and only if $f(x)$ and $f(x) - x$ both appear in the complete list of **PP**s above.

It is not difficult to see that if $f(x)$ is of the form (4.5) then it is not possible for $f(x) - x$ to be of any of the forms (4.5)-(4.9). So there are no orthomorphism polynomials of the form (4.5). Similar reasoning shows that the only possibility for $f(x)$ and $f(x) - x$ to both be on the list is if one is of the form (4.8) and the other is of the form (4.9). First consider the case where $f(x)$ is of the form (4.8). Let

$$f(x) = cx^6 + acx^5 + 2a^3cx^3 + a^4cx^2 + (2+i)a^5cx, \tag{4.10}$$

where $a, c \neq 0$. Then

$$f(x) - x = cx^6 + acx^5 + 2a^3cx^3 + a^4cx^2 + ((2+i)a^5c - 1)x. \tag{4.11}$$

For $f(x) - x$ to be of the form (4.9) we there must exist $A, C \neq 0$ such that

$$f(x) - x = Cx^6 + ACx^5 + 2A^3Cx^3 + A^4Cx^2 + (2-i)A^5Cx. \tag{4.12}$$

Equating coefficients of (4.11) and (4.12) we conclude that $C = c, A = a$ and that

$$(2+i)a^5c - 1 = (2-i)a^5c.$$

Rearranging, we have $c = a^3i$. Substituting this into (4.10) we have

$$f(x) = a^3ix^6 + a^4ix^5 + 2a^6ix^3 + a^7ix^2 + 2(1+i)x$$

Replacing a with $a^{-1}i$ we have

$$f(x) = a^5x^6 + a^4ix^5 + a^2ix^3 + ax^2 + 2(1+i)x.$$

In a similar fashion we determine that $f(x)$ is of the form (4.9) and $f(x) - x$ is of the form (4.8) if and only if

$$f(x) = a^5x^6 - a^4ix^5 - a^2ix^3 + ax^2 + 2(1-i)x.$$

□

Finally we show that there are no degree 6 orthomorphism polynomials of $\mathbb{F}_{3^r}$ for any $r > 2$.

Theorem 4.5. *There are no degree 6 orthomorphism polynomials of* $\mathbb{F}_{3^r}$ *for any* $r > 2$.

Proof. By Theorems 3.15 and 3.17 there are no **PP**s of $\mathbb{F}_{3^r}$ for any $r > 3$, so certainly there are no orthomorphism polynomials.

Let $r = 3$ and let $f(x)$ be a degree 6 orthomorphism polynomial of $\mathbb{F}_{3^3}$. By a linear transformation we may assume that f satisfies (*P1*) and either (*P2*) or (*P3*). By Table 3.1 (9) we then have

$$f(x) = cx^6 + acx^5 + 2a^4cx^2, \tag{4.13}$$

for some $a, c \neq 0$. But clearly $f(x) - x$ cannot also be of the form (4.13), so $f(x) - x$ is not a **PP**, a contradiction. □

By Theorems 4.3 - 4.5 there are degree 6 orthomorphism polynomials of $\mathbb{F}_{3^r}$ if and only if $r = 2$. The following is the classification of degree 6 orthomorphism polynomials of $\mathbb{F}_{3^2}$:

$$ax^6 + a^7x^4 + a^5x^2 + 2x, \quad (a \neq 0) \tag{4.14}$$

$$ax^6 + a^7x^4 - 2^{1/2}a^2x^3 + a^5x^2 + (2 + 2^{1/2})x, \quad (a \neq 0) \tag{4.15}$$

$$a^5x^6 + 2^{1/2}a^4x^5 + 2^{1/2}a^2x^3 + ax^2 + 2(1 + 2^{1/2})x. \quad (a \neq 0) \tag{4.16}$$

Every degree 6 orthomorphism polynomial of $\mathbb{F}_{3^2}$ is of one of the forms

- $f(x) + d$, where $f(x)$ is of the form (4.14) or (4.15) and $d \in \mathbb{F}_{3^2}$, or
- $g(x + b) + d$, where $g(x)$ is of the form (4.16) and $b, d \in \mathbb{F}_{3^2}$.

Appendix A

List of Normalised PPs

With the exception of degree 6 polynomials in even characteristic, the following table is the complete list of normalised permutation polynomials of degree $\leqslant 6$. The reader is referred to the recent paper [13] by Li *et al.* for the classification of **PP**s of degree 6 and 7 over fields of even characteristic.

Normalised **PP**	q
x	any q
x^2	$q \equiv 0 \bmod 2$
x^3	$q \not\equiv 1 \bmod 3$
$x^3 - ax$, a not square	$q \equiv 0 \bmod 3$
$x^4 \pm 3x$	$q = 7$
$x^4 + a_1x^2 + a_2x$, if its only root in $\mathbb{F}_q$ is 0	$q \equiv 0 \bmod 2$
x^5	$q \not\equiv 1 \bmod 5$
$x^5 - ax$, a not a fourth power	$q \equiv 0 \bmod 5$
$x^5 + 2^{1/2}x$	$q = 9$
$x^5 \pm 2x^2$	$q = 7$
$x^5 + ax^3 \pm x^2 + 3a^2x$, a not a square	$q = 7$
$x^5 + ax^3 + 5^{-1}a^2x$, a arbitrary	$q \equiv 2, 3 \bmod 5$
$x^5 + ax^3 + 3a^2x$, a not square	$q = 13$
$x^5 - 2ax^3 + a^2x$, a not square	$q \equiv 0 \bmod 5$
$x^6 \pm 2x$	$q = 11$
$x^6 \pm 4x$	$q = 11$
$x^6 \pm a^2x^3 + ax^2 \pm 5x$, a a nonzero square	$q = 11$
$x^6 \pm 4a^2x^3 + ax^2 \pm 4x$, a not square	$q = 11$
$x^6 + a^2x^4 + a^7bx^3 + a^4x^2 + a(2b+1)x$, $a \neq 0, b \in \{0, 1, 2^{1/2}, 1 + 2^{1/2}\}$	$q = 3^2$
$x^6 + ax^5 + 2abx^4 + (a^3 + ab^2 + 2b^3)x^3 + (2a^4 + ab^3)x^2+$ $(2a^5 + a^4b + 2ab^4)x, a \neq 0$, b arbitrary	$q = 3^2$
$x^6 + ax^5 + 2abx^4 + (ab^2 + 2b^3 + a^3\varphi)x^3 + (ab^3 + 2a^4\varphi)x^2+$ $(2^{1/2}a^5 + 2ab^4 + a^4b\varphi)x, a \neq 0$, b arbitrary, $\varphi = \pm(1 - 2^{1/2})$	$q = 3^2$
$x^6 + ax^5 + 2abx^4 + (2a^3 + ab^2 + 2b^3)x^3 + (a^4 + ab^3)x^2+$ $(2a^5 + 2^{1/2}a^5 + 2a^4b + 2ab^4)x, a \neq 0$, b arbitrary	$q = 3^2$
$x^6 + ax^5 + 2abx^4 + (ab^2 + 2b^3)x^3 + (2a^4 + ab^3)x^2+$ $(a^4b + 2ab^4)x, a \neq 0$, b arbitrary	$q = 3^3$

Table A.1: *List of Normalised Permutation Polynomials.*

Note that in this table $2^{1/2}$ always occurs as a symbol for *either* root of the polynomial $x^2 - 2$ in $\mathbb{F}_{3^2}$.

Bibliography

[1] S. D. Cohen. The distribution of polynomials over finite fields. *Acta Arith.*, 17:255–271, 1970.

[2] S. D. Cohen. Permutation polynomials and primitive permutation groups. *Arch. Math.*, 57:417–423, 1991.

[3] S. D. Cohen and M. D. Fried. Lenstra's proof of the Carlitz-Wan conjecture on exceptional polynomials: an elementary version. *Finite Fields Appl.*, 1:372–375, 1995.

[4] H. Davenport and E. Bombieri. On two problems of Mordell. *Amer. J. Math.*, 88:61–70, 1966.

[5] H. Davenport and D. J. Lewis. Notes on congruences (I). *Quart. J. Math.*, 14:51–60, 1963.

[6] L. E. Dickson. The analytic representation of substitutions on a power of a prime number of letters with a discussion of the linear group, part II. *Ann. of Math*, 11:65–120, 1896-1897.

[7] A. B. Evans. Orthogonal latin squares based on groups. Preprint.

[8] A. B. Evans. *Orthomorphism Graphs of Groups.* Springer, 1992.

[9] M.D. Fried, R. Guralnick, and J. Saxl. Schur covers and Carlitz's conjecture. *Israel J. Math.*, 82:157–225, 1993.

[10] D. R. Hayes. A geometric approach to permutation polynomials over a finite field. *Duke Math. J.*, 34:293–305, 1967.

[11] C. Hermite. Sur les fonctions de sept lettres. *C. R. Acad. Sci. Paris*, 57:750–757, 1854.

[12] H. Lausch and W. Nöbauer. *Algebra of Polynomials.* North-Holland Publishing Co., Amsterdam-London, 1973.

[13] J. Li, D. B. Chandler, and Q. Xiang. Permutation polynomials of degree 6 or 7 over finite fields of characteristic 2. *Finite Fields Appl.*, 16:406419, 2010.

[14] R. Lidl and G. L. Mullen. When does a polynomial over a finite field permute the elements of the field? *Amer. Math. Monthly*, 95:243–246, 1988.

[15] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, second edition, 1997.

[16] C. R. MacCleur. On a conjecture of Davenport and Lewis concerning exceptional polynomials. *Acta. Arith.*, 12:289–299, 1967.

[17] G. L. Mullen. Permutation polynomials over finite fields. In *Finite Fields, Coding Theory and Advances in Communications and Computing*, pages 131–151. Marcel Dekker, 1993.

[18] G. L. Mullen. Permutation polynomials: a matrix analogue of Schur's conjecture and a survey of recent results. *Finite Fields Appl.*, 1:242–258, 1995.

[19] H Niederreiter and K. H. Robinson. Complete mappings of finite fields. *J. Austral. Math. Soc. Ser. A*, 33:197–212, 1982.

[20] G. Raussnitz. Zur theorie der congruenzen höheren grades. *Math. Naturwiss. Ber. Ungarn*, 1:266–278, 1883.

[21] I. E. Shparlinski. A deterministic test for permutation polynomials. *Comput. Complexity*, 2:129–132, 1992.

[22] A. Tietäväinen. On non-residues of a polynomial. *Ann. Univ. Turku. Ser. AI*, 94:6 pp, 1966.

[23] G. Turnwald. A new criterion for permutation polynomials. *Finite Fields Appl.*, 1:64–82, 1995.

[24] J. von zur Gathen. Tests for permutation polynomials. *SIAM J. Comput.*, 20:591–602, 1991.

[25] J. von zur Gathen. Values of polynomials over finite fields. *Bull. Austral. Math. Soc.*, 43:141–146, 1991.

[26] D. Wan. On a problem of Niederreiter and Robinson about finite fields. *J. Austral. Math. Soc. Ser. A*, 41:336–338, 1986.

[27] D. Wan. On a conjecture of Carlitz. *J. Austral. Math. Soc.*, 43:375–384, 1987.

[28] D. Wan. Permutation polynomials and resolution of singularities over finite fields. *Proc. Amer. Math. Soc.*, 110:303–309, 1990.

[29] D. Wan. A generalization of the Carlitz conjecture. In *Finite Fields, Coding Theory and Advances in Communications and Computing*, pages 431–432. Marcel Dekker, 1993.

[30] D. Wan. A p-adic lifting lemma and its applications to permutation polynomials. In *Finite Fields, Coding Theory and Advances in Communications and Computing*, pages 209–216. Marcel Dekker, 1993.

[31] D. Wan. Permutation binomials over finite fields. *Acta Math. Sinica (N.S.)*, 10:30–35, 1994. Special Edition.

[32] D. Wan and R. Lidl. Permutation polynomials of the form $x^r f(x^{(q1)/d})$ and their group structure. *Monatsh. Math.*, 112:149–163, 1991.

[33] C. Wells. The degrees of permutation polynomials over finite fields. *J. Combinatorial Theory*, 7:4955, 1969.

[34] K. S. Williams. On exceptional polynomials. *Canad. Math. Bull.*, 11:279–282, 1968.